Dominion KSX II

User Guide
Release 2.3.0

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Contents

Chapter 4   Rack PDU (Power Strip) Outlet Control   86

Chapter 5   Virtual Media   90

Chapter 6   USB Profiles   104

Chapter 7   User Management   113

Chapter 8   Device Management   135

Chapter 9   Security Management   189

Chapter 10   Maintenance   204

Chapter 11   Diagnostics   219

Chapter 12   Command Line Interface (CLI)   225

Chapter 13 KSX II Local Console 240

Appendix C   Informational Notes   301

Chapter 1   Introduction

In This Chapter

KSX II Overview

Raritan's Dominion KSX II is an enterprise-class, secure digital device that provides a single integrated solution for remote KVM (keyboard, video, mouse) server access and serial device management, as well as power control from anywhere in the world from a web browser. At the rack, the KSX II provides control of all KVM server and serial targets from a single keyboard, monitor, and mouse. Total access and control of all serial targets is also available from a single local serial port. The integrated remote access capabilities of the KSX II provide full access and control of your servers from a web browser.

KSX II is easily installed using standard UTP (Cat 5/5e/6) cabling. Its advanced features include virtual media, up to 256-bit encryption, remote power control, dual Ethernet, LDAP, RADIUS, Active Directory®, Syslog integration, and web management. These features enable you to deliver higher uptime, better productivity, and bulletproof security - any time from anywhere.

KSX II products can operate as standalone devices and do not rely on a central management device. For larger data centers and enterprises, multiple KSX II devices can be integrated into a single logical solution with other Raritan devices using Raritan's CommandCenter Secure Gateway (CC-SG) management unit.
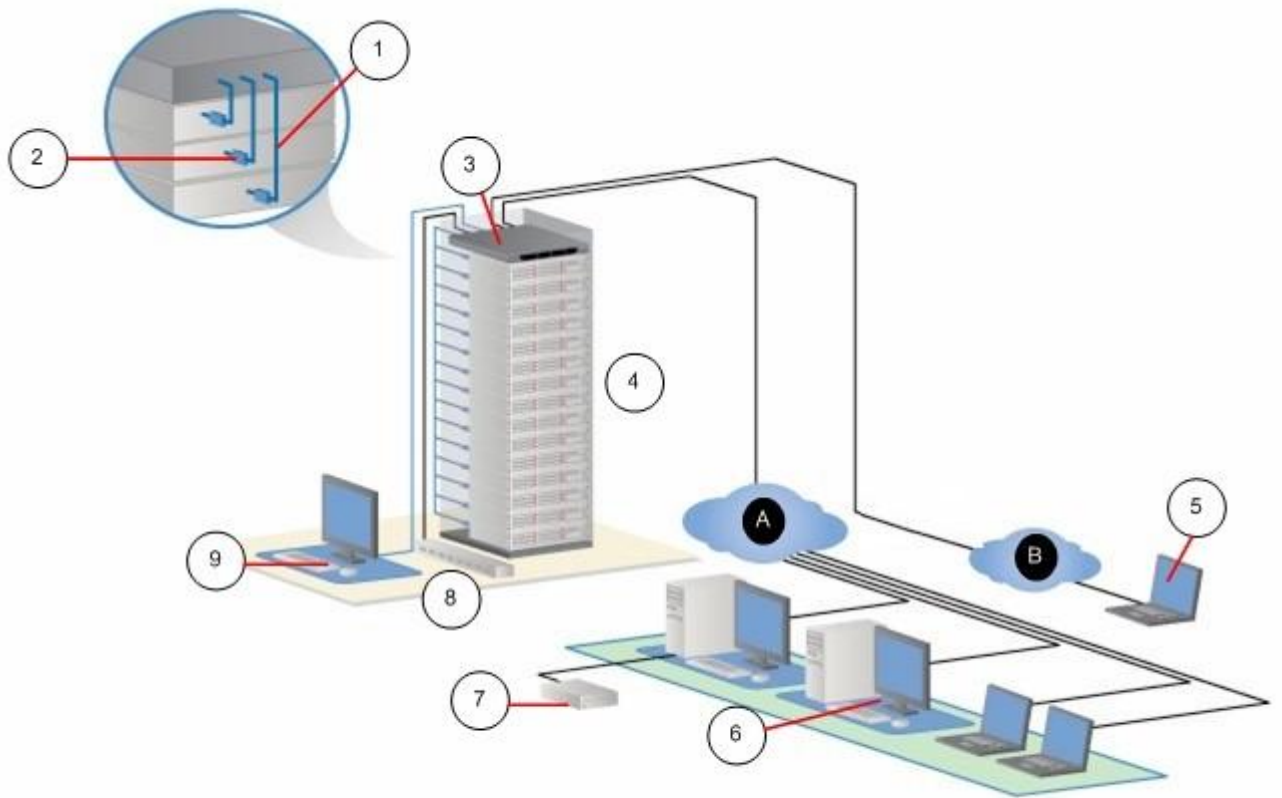
Diagram key			
(1)	Cat5 cable	(7)	Remote virtual media USB drive(s)
(2)	Computer Interface Module (CIM)	(8)	Rack PDU (power strip)
(3)	KSX II	(9)	Local access
(4)	Remote KVM and serial devices	(A)	IP LAN/WAN
(5)	Modem access	(B)	PSTN
(6)	Remote (network) access		

What's New in Help

The following information has been added based on enhancements and changes to the equipment and/or user documentation.

- You are able to configure HTTP and/or HTTPS ports used by the KSX II. See **HTTP and HTTPS Port Settings** (on page 141).

- Information on the new KSX II support for smart card readers has been added to the help. See **Smart Cards** (on page 75), and **Smart Card Readers** (on page 282).

- A security banner feature has been added that allows you to create and display a security banner and optionally require users to accept or decline a security agreement during the KSX II login process. See **Security Banner** (on page 202).

- The KSX II now contains an embedded FIPS 140-2 validated cryptographic module. See **Encryption & Share** (on page 193).

- The KSX II supports the P2CIM-APS2DUAL and P2CIM-AUSBDUAL CIMs, which provide two RJ45 connections to different KVM switches. See **Supported Paragon CIMS and Configurations** (on page 275).

- A Direct Port Access feature that allows you to connect directly to targets from your browser has been added to the KSX II. See **Device Services** (on page 140).

- Active KVM Client is now supported by the KSX II. See **Active KVM Client (AKC)** (on page 80).

- USB profiles are now supported by the KSX II. See **USB Profiles** (on page 104).

- Support for additional widescreen video resolutions has been added to the KSX II. See **Supported Video Resolutions** (on page 279).

- A new tab has been added to the Port Access page that allows you to search for a server by name. See **Port Access Page** (on page 45).

- KSX II now supports Microsoft's Window 7® operating system. See **Supported Operating Systems (Clients)** (on page 270) and **Supported Operating Systems and CIMs (KVM Target Servers)** (on page 271).

- You can now log a user off (force logoff). See **Logging a User Off (Force Logoff)** (on page 122).

Please see the release notes for a more detailed explanation of the changes applied to the device and this version of the help.

KSX II Help

The KSX II help provides information on how to install, set up, and configure the KSX II. It also includes information on accessing target servers and power strips, using virtual media, managing users and security, and maintaining and diagnosing the KSX II.

A PDF version of the help can be downloaded from the *Raritan Firmware and Documentation page http://www.raritan.com/support/firmware-and-documentation/* on the Raritan website. Raritan recommends that you refer to the Raritan website for the most up-to-date user guides available.

To use online help, Active Content must be enabled in your browser. If you are using Internet Explorer 7, you must enable Scriplets. Consult your browser help for information on enabling these features.

Related Documentation

The KSX II help is accompanied by a KSX II Device Quick Setup Guide, which can be found on the *Raritan Firmware and Documentation page http://www.raritan.com/support/firmware-and-documentation/* of Raritan's website.

Installation requirements and instructions for client applications used with the KSX II can be found in the **KVM and Serial Access Clients Guide**, also found on the Raritan website. Where applicable, specific client functions used with the KSX II are included in the help.

KSX II Client Applications

The following client applications can be used with the KSX II:

- Virtual KVM Client (VKC)
- Active KVM Client (AKC)
- Multiplatform Client (MPC)
- Raritan Serial Console (RSC)

See the **KVM and Serial Client Guide** for additional information on the client applications. Also see the *Working with Target Servers* (on page 38) section of this guide, which contains information on using the clients with the KSX II.

Note: MPC and VKC require the Java™ Runtime Environment (JRE™). AKC is .NET based.

Virtual Media

All KSX II models support virtual media. The benefits of virtual media - mounting of remote drives/media on the target server to support software installation and diagnostics - are now available in all of the KSX II models. Virtual media sessions can be secured by using 128-bit and 256-bit AES or RC4 encryption.

Each KSX II comes equipped with virtual media to enable remote management tasks using the widest variety of CD, DVD, USB, internal and remote drives, and images. Unlike other solutions, the KSX II supports virtual media access of hard drives and remotely mounted images for added flexibility and productivity.

The new D2CIM-VUSB and D2CIM-DVUSB CIMs (computer interface module) support virtual media sessions to KVM target servers supporting the USB 2.0 interface. This new CIM also supports Absolute Mouse Synchronization as well as remote firmware updates.

Note: The black connector on the DVUSB CIM is used for keyboard and mouse. The gray connector is used for virtual media. Keep both plugs of the CIM connected to the device. The device may not operate properly if both plugs are not connected to the target server.

Product Photos

KSX II 144 and 188

CIM   *Serial Adapter*

Product Features

Hardware

- KVM and serial remote access over IP
- 1U rack-mountable; brackets included
- DKSX2-144 - 4 serial/4 KVM server ports
- DKSX2-188 - 8 serial/8 KVM server ports
- 1 KVM channel shareable by 8 users, multiple serial users.
- UTP (Cat5/5e/6) server cabling
- Dual Ethernet ports (10/100/1000 LAN) with failover
- Field upgradeable
- Local KVM port for in-rack access
    - PS/2 keyboard/mouse ports
    - One front and three back panel USB 2.0 ports for supported USB devices
    - Fully concurrent with remote user access
    - Local Graphical User Interface (GUI) for administration
    - Both KVM and serial targets can be connected using KVM local port
- Local serial port (RS232) for CLI-based administration and serial target access
- Integrated power control
- Dual dedicated power control ports
- LED indicators for network activity, and remote KVM user status
- Hardware reset button
- Internal modem
- Centralized access security

Software

- Virtual media with D2CIM-VUSB and D2CIM-DVUSB CIMs

- Absolute Mouse Synchronization with D2CIM-VUSB CIM and D2CIM-DVUSB CIMs

- Plug-and-Play

- Web-based access and management

- Intuitive Graphical User Interface (GUI)

- 256-bit encryption of complete KVM signal, including video and virtual media

- LDAP/LDAPS, Active Directory®, RADIUS, or internal with local authentication and authorization

- DHCP or fixed IP addressing

- Smart card/CAC authentication

- SNMP and Syslog management

- IPv4 and IPv6 support

- Power control associated directly with servers to prevent mistakes

- Integration with Raritan's CommandCenter Secure Gateway (CC-SG) management unit

- CC Unmanage feature to remove the device from CC-SG control

External Product Overview

The following diagram indicates the external components of the KSX II. Note that the KSX II 144 will have 4 KVM ports and 4 serial ports as compared to the KSX II 188 used in the diagram, which has 8 KVM ports and 8 serial ports.

Item	Description
A	USB port
B	Remote indicator light
C	LAN1 and LAN2 indicator lights
D	Power indicator light
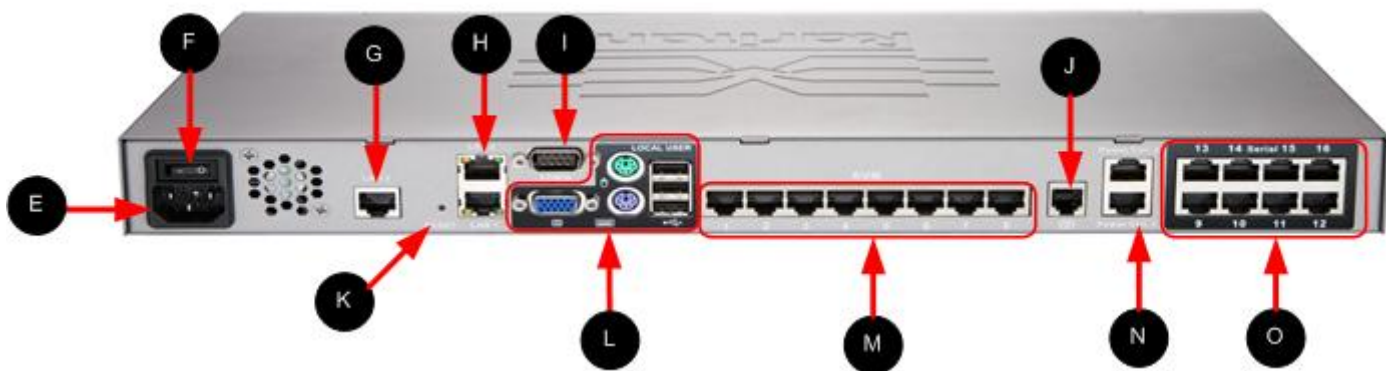
Item	Description
E	AC power cord plug
	See **Power Control** (on page 158) for additional information.
F	Power on/off switch
G	LAN 3 port
	Note: The LAN 3 port is reserved for future use.
H	LAN1 and LAN2 ports
	See **Step 3: Connect the Equipment** (on page 25) for additional information.
I	Admin port
	See **Step 3: Connect the Equipment** (on page 25) for additional information.
J	External modem port
	See **Modem Configuration** (on page 256) for additional information.
K	Reset button
	See **Resetting the KSX II Using the Reset Button** (on page 254) for additional information.
L	Local port
	See **Step 3: Connect the Equipment** (on page 25) for additional information.
M	KVM ports
	See **Step 3: Connect the Equipment** (on page 25) for additional information.
N	Power Ctrl. 1 and Power Ctrl. 2
	See **Power Control** (on page 158) for additional information.
O	Serial ports
	See **Step 3: Connect the Equipment** (on page 25) for additional information.

Terminology

This manual uses the following terminology for the components of a typical KSX II configuration:

Diagram key	
1	**TCP/IP** IPv4 and/or IPv6
2	**KVM (Keyboard, Video, Mouse)**
3	**UTP Cable (Cat5/5e/6)**
A	**KSX II**
B	**Local Access Console** Local User - an optional user console (consisting of a keyboard, mouse, and multi-sync VGA monitor) attached directly to the KSX II to control KVM target servers and serial targets locally (directly at the rack, not through the network). A USB smart card reader can also be attached at the Local port to mount onto a target server. Local Administrator - use the Local Administrator port to connect the KSX II directly to a workstation to manage your serial targets and configure the system with a terminal emulation program such as HyperTerminal. The Local Administrator port requires the use of a standard null modem cable.
C	**Remote PC** Networked computers used to access and control KVM target servers and serial targets connected to the KSX II. Refer to Supported Operating Systems (Clients) for a list of the Operating Systems supported by the KSX II remotely.
D	**CIMs** Dongles that connect to each target server. Available for all of the supported Operating Systems. Refer to Supported CIMs for information about the CIMs supported by the KSX II.
E	**Serial Adapter** Adapters that connect serial cables.
F	**Target Servers** KVM Target Servers - servers with video cards and user interfaces (for example, Windows®, Linux®, Solaris™, and so forth) connected remotely via the KSX II. Refer to Supported Operating Systems and CIMs (Target Servers) for a list of the supported Operating Systems and CIMs. Serial Targets - Servers, routers, and switches that have a

Diagram key	
	serial port connected remotely via KSX II.
G	**Routers**
H	**Dominion PX Rack PDU (Power Strip)** Raritan rack PDUs accessed remotely via the KSX II.

Package Contents

Each KSX II ships as a fully-configured stand-alone product in a standard 1U 19" rackmount chassis. Each KSX II device ships with the following contents:

Amount included	Item
1	Dominion KSX II device
1	Dominion KSX II Quick Setup Guide
1	Rackmount Kit
1	AC Power Cord
1	Cat5 Network Cable
1	Cat5 Network Crossover Cable
1	Set of 4 Rubber Feet (for desktop use)
1	Application Note
1	Warranty Card
1	Phone Line Cable
1	Loopback Adapter

Chapter 2   Installation and Configuration

In This Chapter

Overview

This section provides a brief overview of the installation process. Each step is further detailed in the remaining sections of this chapter.

▶   **To install and configure the KSX II:**

- *Step 1: Configure KVM Target Servers* (on page 15)

- *Step 2: Configure Network Firewall Settings* (on page 24)

- *Step 3: Connect the Equipment* (on page 25)

- *Step 4: Configure the KSX II* (on page 30)

- *Step 5 (Optional): Configure Keyboard Language* (on page 37)

You will need to know the default IP address, username, and password for initial configuration. See *Default Login Information* (on page 14).

Default Login Information

Default	Value
User name	The default user name is admin. This user has administrative privileges.
Password	The default password is raritan.
	Passwords are case sensitive and must be entered in the exact case combination in which they were created. For example, the default password raritan must be entered entirely in lowercase letters.
	The first time you start the KSX II, you are required to change the default password.
IP address	The KSX II ships with the default IP address of 192.168.0.192.
Important: For backup and business continuity purposes, it is strongly recommended that you create a backup administrator user name and password and keep that information in a secure location.	

Getting Started

Step 1: Configure KVM Target Servers

KVM target servers are the computers that will be accessed and controlled via the KSX II. Before installing the KSX II, configure all KVM target servers to ensure optimum performance. This configuration applies only to KVM target servers, not to the client workstations (remote PCs) used to access the KSX II remotely. See **Terminology** for additional information.

Desktop Background

For optimal bandwidth efficiency and video performance, KVM target servers running graphical user interfaces such as Windows®, Linux®, X-Windows, Solaris™, and KDE require configuration. The desktop background need not be completely solid but desktop backgrounds featuring photos or complex gradients might degrade performance.

Mouse Settings

The KSX II operates in several mouse modes:

- Absolute Mouse Mode™ (D2CIM-VUSB only)
- Intelligent Mouse Mode (do not use an animated mouse)
- Standard Mouse Mode

Mouse parameters do not have to be altered for Absolute Mouse Synchronization but D2CIM-VUSB or D2CIM-DVUSB is required for this mode. For both the Standard and Intelligent mouse modes, mouse parameters must be set to specific values, which are described here. Mouse configurations will vary on different target operating systems. Consult your OS documentation for additional detail.

Intelligent mouse mode generally works well on most Windows platforms. Intelligent mouse mode may produce unpredictable results when active desktop is set on the target. For additional information on Intelligent mouse mode settings, see **Intelligent Mouse Mode** (on page 72).

Servers with internal KVM switches inside the blade chassis typically do not support absolute mouse technology.

Operating System Mouse and Video Settings

This section provides video mode and mouse information specific to the operating system in use on the target server.

Windows XP, Windows 2003 and Windows 2008 Settings

▶ **To configure KVM target servers running Windows XP®, Windows 2003® and Windows 2008®:**

1. Configure the mouse settings:

   a. Choose Start > Control Panel > Mouse.

   b. Click the Pointer Options tab.

   c. In the Motion group:

      ▪ Set the mouse motion speed setting to exactly the middle speed.

      ▪ Disable the "Enhance pointer precision" option.

      ▪ Disable the Snap To option.

      ▪ Click OK.

2. Disable transition effects:

   a. Select the Display option from the Control Panel.

   b. Click the Appearance tab.

      ▪ Click the Effects button.

      ▪ Deselect the "Use the following transition effect for menus and tooltips" option.

3. Click OK and close the Control Panel.

Note: For KVM target servers running Windows XP, Windows 2000 or Windows 2008, you may wish to create a user name that will be used only for remote connections through the KSX II. This will enable you to keep the target server's slow mouse pointer motion/acceleration settings exclusive to the KSX II connection.

Windows XP, 2000, and 2008 login pages revert to preset mouse parameters that differ from those suggested for optimal KSX II performance. As a result, mouse synchronization may not be optimal for these screens.

WARNING! Proceed only if you are comfortable adjusting the registry on Windows KVM target servers. You can obtain better KSX II mouse synchronization at the login pages by using the Windows registry editor to change the following settings: HKey_USERS\.DEFAULT\Control Panel\Mouse: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0.

Windows Vista Settings

▶ **To configure KVM target servers running Windows Vista®
operating system:**

1. Configure the mouse settings:

    a. Choose Start > Settings > Control Panel > Mouse.

    b. Select "Advanced system settings" from the left navigation panel.
        The System Properties dialog opens.

    c. Click the Pointer Options tab.

    d. In the Motion group:

        ▪ Set the mouse motion speed setting to exactly the middle
          speed.

        ▪ Disable the "Enhanced pointer precision" option.

        ▪ Click OK.

2. Disable animation and fade effects:

    a. Select the System option from the Control Panel.

    b. Select Performance Information then Tools > Advanced Tools >
        Adjust to adjust the appearance and performance of Windows.

    c. Click the Advanced tab.

    d. Click the Settings button in the Performance group to open the
        Performance Options dialog.

    e. Under Custom options, deselect the following checkboxes:

    ▪ Animation options:

        ▪ Animate controls and elements inside windows

        ▪ Animate windows when minimizing and maximizing

    ▪ Fade options:

        ▪ Fade or slide menus into view

        ▪ Fade or slide ToolTips into view

        ▪ Fade out menu items after clicking

3. Click OK and Close the Control Panel.

▶ **To configure KVM target servers running Windows 7® operating
system:**

1. Configure the mouse settings:

    a. Choose Start > Control Panel > Hardware and Sound > Mouse.

    b. Click the Pointer Options tab.

    c. In the Motion group:

- Set the mouse motion speed setting to exactly the middle speed.

- Disable the "Enhanced pointer precision" option.

- Click OK.

2. Disable animation and fade effects:

   a. Select Control Panel > System and Security.

   b. Select System and then select "Advanced system settings" from the left navigation panel. The System Properties dialog appears.

   c. Click the Advanced tab.

   d. Click the Settings button in the Performance group to open the Performance Options dialog.

   e. Under Custom options, deselect the following checkboxes:

   - Animation options:

     - Animate controls and elements inside windows

     - Animate windows when minimizing and maximizing

   - Fade options:

     - Fade or slide menus into view

     - Fade or slide ToolTips into view

     - Fade out menu items after clicking

3. Click OK and Close the Control Panel.

Windows 2000 Settings

▶ **To configure KVM target servers running Microsoft Windows 2000® operating system:**

1. Configure the mouse settings:

   a. Choose Start > Control Panel > Mouse.

   b. Click the Motion tab.

      - Set the acceleration to None.

      - Set the mouse motion speed setting to exactly the middle speed.

      - Click OK.

2. Disable transition effects:

   a. Select the Display option from the Control Panel.

   b. Click the Effects tab.

▪ Deselect the "Use the following transition effect for menus and tooltips" option.

3. Click OK and close the Control Panel.

Linux Settings (Red Hat 4)

Note: The following settings are optimized for Standard Mouse mode only.

▶ **To configure KVM target servers running Linux® (graphical user interface):**

1. Configure the mouse settings:

   a. Red Hat 5 users, choose Main Menu > Preferences > Mouse. Red Hat 4 users, choose System > Preferences > Mouse. The Mouse Preferences dialog appears.

   b. Click on the Motion tab.

   c. Within the Speed group, set the Acceleration slider to the exact center.

   d. Within the Speed group, set the Sensitivity towards low.

   e. Within the Drag & Drop group, set the Threshold towards small.

   f. Close the Mouse Preferences dialog.

Note: If these steps do not work, issue the xset mouse 1 1 command as described in the Linux command line instructions.

2. Configure the screen resolution:

   a. Choose Main Menu > System Settings > Display. The Display Settings dialog appears.

   b. On the Settings tab, select a Resolution supported by the KSX II.

   c. Click OK.

Note: Once connected to the target server, in many Linux graphical environments, the <Ctrl> <Alt> <+> command will change the video resolution, scrolling through all available resolutions that remain enabled in the XF86Config or /etc/X11/xorg.conf, depending on your X server distribution

Note: If you change the video resolution, you must log out of the target server and log back in for the video settings to take effect.

SUSE Linux 10.1 Settings

Note: Do not attempt to synchronize the mouse at the SUSE Linux® login prompt. You must be connected to the target server to synchronize the mouse cursors.

▶ **To configure the mouse settings:**

1. Choose Desktop > Control Center. The Desktop Preferences dialog appears.

2. Click Mouse. The Mouse Preferences dialog appears.

3. Open the Motion tab.

4. Within the Speed group, set the Acceleration slider to the exact center position.

5. Within the Speed group, set the Sensitivity slider to low.

6. Within the Drag & Drop group, set the Threshold slider to small.

7. Click Close.

▶ **To configure the video:**

1. Choose Desktop Preferences > Graphics Card and Monitor. The Card and Monitor Properties dialog appears.

2. Verify that a Resolution and Refresh Rate is in use that is supported by the KSX II. See **Supported Video Resolutions** (on page 279) for more information.

   Note: If you change the video resolution, you must log out of the target server and log back in for the video settings to take effect.

Make Linux Settings Permanent

Note: These steps may vary slightly depending on the specific version of Linux® in use.

▶ **To make your settings permanent in Linux (prompt):**

1. Choose System Menu > Preferences > Personal > Sessions.

2. Click the Session Options tab.

3. Select the "Prompt on log off" checkbox and click OK. This option prompts you to save your current session when you log out.

4. Upon logging out, select the "Save current setup" option from the dialog.

5. Click OK.

Tip: If you do not want to be prompted upon log out, follow these procedures instead.

▶ **To make your settings permanent in Linux (no prompt):**

1. Choose Desktop > Control Center > System > Sessions.

2. Click the Session Options tab.

3. Deselect the "Prompt on the log off" checkbox.

4. Select the "Automatically save changes to the session" checkbox and click OK. This option automatically saves your current session when you log out.

Make UNIX Settings Permanent

Note: These steps may vary slightly depending on the type of UNIX® (for example, Solaris™, IBM® AIX™) and the specific version in use.

1. Choose Style Manager > Startup. The Style Manager - Startup dialog appears.

2. On the Logout Confirmation dialog, select the On option. This option prompts you to save your current session when you log out.

Sun Solaris Settings

▶ **To configure KVM target servers running Sun™ Solaris™:**

1. Set the mouse acceleration value to exactly 1 and the threshold to exactly 1. This can be performed from:

   ▪ The graphical user interface.
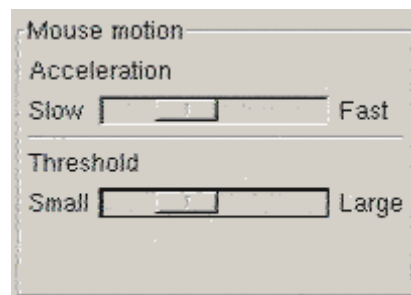
   ▪ The command line *xset mouse a t* where *a* is the acceleration and *t* is the threshold.

2. All KVM target servers must be configured to one of the display resolutions supported by the KSX II. The most popular supported resolutions for Sun machines are:

Display resolution	Vertical refresh rate	Aspect ratio
1600 x 1200	60 Hz	4:3

Display resolution	Vertical refresh rate	Aspect ratio
1280 x 1024	60,75,85 Hz	5:4
1152 x 864	75 Hz	4:3
1024 x 768	60,70,75,85 Hz	4:3
800 x 600	56,60,72,75,85 Hz	4:3
720 x 400	85 Hz	9:5
640 x 480	60,72,75,85 Hz	4:3

3. KVM target servers running the Solaris operating system must output VGA video (H-and-V sync, not composite sync).

▶ **To change your Sun video card output from composite sync to the nondefault VGA output:**

1. Issue the Stop+A command to drop to bootprom mode.

2. Issue the following command to change the output resolution: *setenv output-device screen:r1024x768x70*

3. Issue the `boot` command to reboot the server.

You can also contact your Raritan representative to purchase a video output adapter:

If you have:	Use this video output adapter:
Sun 13W3 with composite sync output	APSSUN II Guardian converter
Sun HD15 with composite sync output	1396C converter to convert from HD15 to 13W3 and an APSSUN II Guardian converter to support composite sync
Sun HD15 with separate sync output	APKMSUN Guardian converter

Note: Some of the standard Sun background screens may not center precisely on certain Sun servers with dark borders. Use another background or place a light colored icon in the upper left hand corner.

Mouse Settings

▶ **To configure the mouse settings (Sun Solaris 10.1):**

1. Choose Launcher. Application Manager - Desktop Controls opens.

2. Choose Mouse Style Manager. The Style Manager - Mouse dialog appears.

3. Set the Acceleration slider to 1.0.

4. Set the Threshold slider to 1.0.

5. Click OK.

Accessing the Command Line

1. Right click.

2. Choose Tools > Terminal. A terminal window opens. (It is best to be at the root to issue commands.)

Video Settings (POST)

Sun systems have two different resolution settings: a POST resolution and a GUI resolution. Run these commands from the command line.

Note: 1024x768x75 is used as an example here; substitute the resolution and refresh rate you are using.

▶ **To check current POST resolution:**

- Run the following command as the root: `# eeprom output-device`

▶ **To change POST resolution:**

1. Run `# eeprom output-device=screen:r1024x768x75`.

2. Log out or restart computer.

Video Settings (GUI)

The GUI resolution can be checked and set using different commands depending on the video card in use. Run these commands from the command line.

Note: 1024x768x75 is used as an example here; substitute the resolution and refresh rate you are using.

Card	To check resolution:	To change resolution:
32-bit	# /usr/sbin/pgxconfig -prconf	1. # /usr/sbin/pgxconfig -res 1024x768x75 2. Log out or restart computer.
64-bit	# /usr/sbin/m64config -prconf	1. # /usr/sbin/m64config -res 1024x768x75 2. Log out or restart computer.
32-bit and 64-bit	# /usr/sbin/fbconfig -prconf	1. # /usr/sbin/fbconfig -res 1024x768x75 2. Log out or restart computer.

IBM AIX 5.3 Settings

Follow these steps to configure KVM target servers running IBM® AIX™ 5.3.

▶ **To configure the mouse:**

1. Go to Launcher.

2. Choose Style Manager.

3. Click Mouse. The Style Manager - Mouse dialog appears.

4. Use the sliders to set the Mouse acceleration to 1.0 and Threshold to 1.0.

5. Click OK.

▶ **To configure the video:**

1. From the Launcher, select Application Manager.

2. Select System_Admin.

3. Choose Smit > Devices > Graphic Displays > Select the Display Resolution and Refresh Rate.

4. Select the video card in use.

5. Click List. A list of display modes is presented.

6. Select a resolution and refresh rate supported by the KSX II. See **Supported Video Resolutions** (on page 279) for more information.

Note: If you change the video resolution, you must log out of the target server and log back in for the video settings to take effect.

Apple Macintosh Settings

For KVM target servers running an Apple Macintosh® operating system, the preferred method is to use the D2CIM-VUSB and Absolute Mouse Synchronization.

Note: 'USB Profile 'Mac OS-X, version 10.4.9 and later' must be selected from the USB Profile menu or the Port Configuration page.

Step 2: Configure Network Firewall Settings

To access KSX II through a network firewall via Multi-Platform Client or through the Port Access page, your firewall must allow communication on TCP Port 5000 or another port that you designate.

To take advantage of the KSX II:	The firewall must allow inbound communication on:
Web-access capabilities	Port 443 - standard TCP port for HTTPS communication
Automatic redirection of HTTP requests to HTTPS (so the more common "http://xxx.xxx.xxx.xxx" can be used instead of "https://xxx.xxx.xxx.xxx")	Port 80 - standard TCP port for HTTP communication

See **Network Settings** (on page 135) for additional information about designating another discovery port.

Step 3: Connect the Equipment

Connect the KSX II to the power supply, network, local PC, KVM target servers, and serial targets.
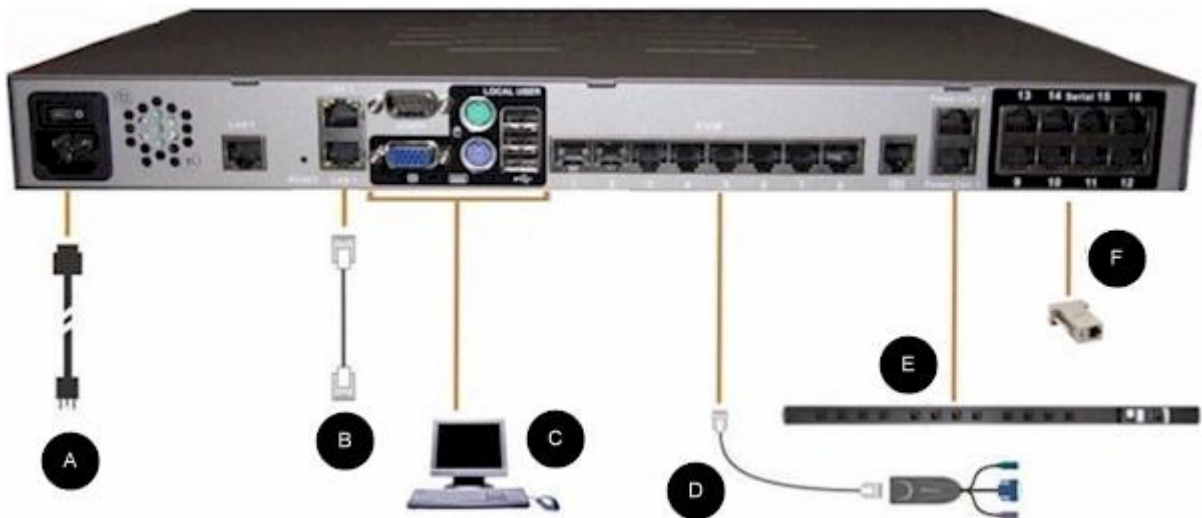
A. AC Power

▶ **To connect the power supply:**

1. Attach the included AC power cord to the KSX II and plug into an AC power outlet.

B. Network Port

The KSX II provides two Ethernet ports for failover purposes (not for load-balancing). By default, only LAN1 is active and the automatic failover is disabled. When enabled, if the KSX II internal network interface or the network switch to which it is connected becomes unavailable, LAN2 will be enabled using the same IP address.

Note: Because a failover port is not activated until after a failover has actually occurred, Raritan recommends that you either not monitor the failover port or monitor it only after a failover occurs.

▶ **To connect the network:**

1. Connect a standard Ethernet cable (included) from the network port labeled LAN1 to an Ethernet switch, hub, or router.

2. To make use of the optional KSX II Ethernet failover capabilities:

   ▪ Connect a standard Ethernet cable from the network port labeled LAN2 to an Ethernet switch, hub, or router.

   ▪ Enable Automatic Failover on the Network Configuration page.

Note: Use both network ports only if you want to use one as a failover port.

C. Local User Port (Local PC) and Local Admin Port

For convenient access to KVM target servers and serial devices while at the rack, use the KSX II Local Access port. While the local port is required for installation and setup, it is optional for subsequent use. The local port provides the KSX II Local Console graphical user interface for administration and target server access.

▶ **To connect the Local User port:**

- Attach a multi-sync VGA monitor, keyboard, and mouse to the respective Local User ports (using either a PS/2 or USB keyboard and mouse).

Connection	Description
Monitor	Attach a standard multi-sync VGA monitor to the HD15 (female) video port.
Keyboard	Attach either a standard PS/2 keyboard to the Mini-DIN6 (female) keyboard port, or a standard USB keyboard to one of the USB Type A (female) ports.

Connection	Description
Mouse	Attach either a standard PS/2 mouse to the Mini-DIN6 (female) mouse port or a standard USB mouse to one of the USB Type A (female) ports.

You can use the Local Admin port to connect the KSX II directly to a workstation to manage your serial targets and configure the system with a terminal emulation program such as HyperTerminal. The Local Admin port requires the use of a standard null modem cable.

Note: When local Authorization and Authentication is set to None, logging in to serial admin console requires username input.

D. KVM Target Server Ports

The KSX II uses standard UTP cabling (Cat5/5e/6) to connect to each target server. Refer to **Specifications** (on page 269) for additional information.

▶ **To connect a KVM target server to the KSX II:**

1. Use the appropriate Computer Interface Module (CIM).   Refer to **Supported Operating Systems and CIMs (KVM Target Servers)** (on page 271) for more information about the CIMs to use with each operating system.

2. Attach the HD15 video connector of your CIM to the video port of your KVM target server. Ensure that your target server's video has already been configured to a supported resolution and refresh rate. For Sun servers, also ensure that your target server's video card has been set to output standard VGA (H-and-V sync) and not composite sync.

3. Attach the keyboard/mouse connector of your CIM to the corresponding ports on your target server. Using a standard straight-through UTP (Cat5/5e/6) cable, connect the CIM to an available server port on the back of your KSX II device.

Note: The DCIM-USB G2 provides a small slide switch on the back of the CIM. Move the switch to P for PC-based USB target servers. Move the switch to S for Sun USB target servers.

A new switch position takes effect only after the CIM is power-cycled. To power-cycle the CIM, remove the USB connector from the target server and plug it back in a few seconds later.

E. Rack PDU (Power Strip)

▶ **To connect the Dominion PX to the KSX II:**

1. Plug one end of a Cat5 cable into the Serial port on the front of the Dominion PX.

2. Connect the other end of the Cat5 cable to either the Power Ctrl. 1 or Power Ctrl. 2 ports on the back of the KSX II.

3. Attach an AC power cord to the target server and an available rack PDU outlet.

4. Connect the rack PDU to an AC power source.

5. Power on the KSX II device.

Important: When using CC-SG, the power ports should be inactive before attaching rack PDUs that were swapped between the power ports. If this is not done, there is a possibility that the number of power outlets will not be correctly detected, especially after swapping 8 and 20 outlet rack PDU models.

Diagram key

A	KSX II	D	PX serial port
B	KSX II Power Ctrl. 1 Port or Power Ctrl. 2 Port	1	Cat5 cable
C	PX		

F. Serial Target Ports

To connect a serial target to the KSX II, use a Cat5 cable with an appropriate serial adapter.

The following table lists the necessary KSX II hardware (adapters and/or cables) for connecting the KSX II to common vendor/model combinations.

Vendor	Device	Console connector	Serial connection
Checkpoint	Firewall	DB9M	ASCSDB9F adapter and a CAT 5 cable
Cisco	PIX Firewall		
Cisco	Catalyst	RJ-45	CRLVR-15 rollover cable; or CRLVR-1 adapter cable and a CAT5 cable

CRLVR-1 cable for connecting a terminal port (RJ-45 Connector type) of KSX II-48 models that have this connector to another KSX II. |
Cisco	Router	DB25F	ASCSDB25M adapter and a CAT 5 cable
Hewlett Packard®	UNIX® Server	DB9M	ASCSDB9F adapter and a CAT 5 cable
Silicon	Origin		

Vendor	Device	Console connector	Serial connection
Graphics			
Sun™	SPARCStation	DB25F	ASCSDB25M adapter and a CAT 5 cable
Sun	Netra T1	RJ-45	CRLVR-15 cable; or CRLVR-1 adapter and a CAT5 cable
Sun	Cobalt	DB9M	ASCSDB9F adapter and a CAT 5 cable
Various	Windows NT®		

Go to the Support page on Raritan's website (www.raritan.com) to obtain a list of commonly used cables and adapters.

Step 4: Configure the KSX II

The first time you power up the KSX II device, there is some initial configuration that you need to perform through the KSX II Local Console:

- Change the default password.
- Assign the IP address.
- Name the KVM target servers.

Changing the Default Password

The KSX II ships with a default password. The first time you start the KSX II you are required to change that password.

▶ **To change the default password:**

1. Power on the KSX II using the power switch(s) at the back of the unit. Wait for the KSX II unit to boot. (A beep signals that the boot is complete.)

2. Once the unit has booted, the KSX II Local Console is visible on the monitor attached to the KSX II local port. Type the default username (admin) and password (raritan) and click Login. The Change Password screen is displayed.

3. Type your old password (raritan) in the Old Password field.

4. Type a new password in the New Password field and retype the new password in the Confirm New Password field. Passwords can be up to 64 characters in length and can consist of English, alphanumeric characters as well as special characters.

5. Click Apply.

6. You will receive confirmation that the password was successfully changed. Click OK. The Port Access page is displayed.

Note: The default password can also be changed from the Raritan Multi-Platform Client (MPC). For more information, refer to Changing a Password.

Assigning an IP Address

These procedures describe how to assign an IP address on the Network Settings page. For complete information about all of the fields and the operation of this page, see **Network Settings**.

▶ **To assign an IP address:**

1. Choose Device Settings > Network. The Network Settings page opens.

2. Specify a meaningful Device Name for your KSX II device. Up to 32 alphanumeric characters using valid special characters and no spaces.

3. In the IPv4 section, enter or select the appropriate IPv4-specific network settings:

    a. Enter the IP Address if needed. The default IP address is 192.168.0.192.

    b. Enter the Subnet Mask. The default subnet mask is 255.255.255.0.

    c. Enter the Default Gateway if None is selected from the IP Auto Configuration drop-down.

    d. Enter the Preferred DHCP Host Name if DHCP is selected from the IP Auto Configuration drop-down.

    e. Select the IP Auto Configuration. The following options are available:

    ▪   None (Static IP) - This option requires that you manually specify the network parameters.

        This is the recommended option because the KSX II is an infrastructure device and its IP address should not change.

    ▪   DHCP - Dynamic Host Configuration Protocol is used by networked computers (clients) to obtain unique IP addresses and other parameters from a DHCP server.

        With this option, network parameters are assigned by the DHCP server. If DHCP is used, enter the Preferred host name (DHCP only). Up to 63 characters.

4. If IPv6 is to be used, enter or select the appropriate IPv6-specific network settings in the IPv6 section:

    a.   Select the IPv6 checkbox to activate the fields in the section.

    b.   Enter a Global/Unique IP Address. This is the IP address assigned to the KSX II.

    c.   Enter the Prefix Length. This is the number of bits used in the IPv6 address.

    d.   Enter the Gateway IP Address.

    e.   Link-Local IP Address. This address is automatically assigned to the device. It is used for neighbor discovery or when no routers are present. **Read-Only**

    f.   Zone ID. This identifies the device with which the address is associated. **Read-Only**

    g.   Select the IP Auto Configuration. The following options are available:

- None - Use this option if you do not want an auto IP configuration and prefer to set the IP address yourself (static IP). This is the default and recommended option.

  If None is selected for the IP auto configuration, the following Network Basic Settings fields are enabled: Global/Unique IP Address, Prefix Length, and Gateway IP Address allowing you to manually set the IP configuration.

- Router Discovery - Use this option to automatically assign IPv6 addresses that have Global or Unique Local significance beyond that of the Link Local, which only applies to a directly connected subnet.

5. Select Obtain DNS Server Address Automatically if DHCP is selected and Obtain DNS Server Address is enabled. When Obtain DNS Server Address Automatically, the DNS information provided by the DHCP server will be used.

6. If Use the Following DNS Server Addresses is selected, regardless of whether DHCP is selected or not, the addresses entered in this section will be used to connect to the DNS server.

   Enter the following information if the Following DNS Server Addresses option is selected. These addresses are the primary and secondary DNS addresses that will be used if the primary DNS server connection is lost due to an outage.

   a.   Primary DNS Server IP Address

   b.   Secondary DNS Server IP Address

7. When finished, click OK. Your KSX II device is now network accessible.

See *LAN Interface Settings* (on page 138) for information in configuring this section of the Network Settings page.

Note: In some environments, the default LAN Interface Speed & Duplex setting Autodetect (autonegotiator) does not properly set the network parameters, which results in network issues. In these instances, setting the KSX II LAN Interface Speed & Duplex field to 100 Mbps/Full Duplex (or whatever option is appropriate to your network) addresses the issue. See the **Network Settings** *(on page 135) page for more information.*

Naming Target Servers

▶ **To name the target servers:**

1. Connect all of the target servers if you have not already done so. See **Step 3: Connect the Equipment** for a description of connecting the equipment.

2. Using the KSX II Local Console, choose Device Settings > Port Configuration. The Port Configuration page opens.

3. Click the Port Name of the target server you want to rename. The Port Page opens.

4. Assign a name to identify the server connected to that port. The name can be up to 32 characters, and alphanumeric and special characters are allowed.

5. Click OK.

Valid Special Characters for Target Names

Character	Description	Character	Description
!	Exclamation point	;	Semi-colon
"	Double quote	=	Equal sign
#	Pound sign	>	Greater than sign
$	Dollar sign	?	Question mark
%	Percent sign	@	At sign
&	Ampersand	[	Left bracket
(	Left parenthesis	\	Backward slash
)	Right parenthesis	]	Right bracket
*	Asterisk	^	Caret
+	Plus sign	_	Underscore
,	Comma	`	Grave accent
-	Dash	{	Left brace

Character	Description	Character	Description
.	Period	|	Pipe sign
/	Forward slash	}	Right brace
<	Less than sign	~	Tilde
:	Colon		

Configuring Direct Port Access via Telnet, IP Address or SSH

The information in this topic is specific to enabling direct port access for serial targets. Use the Enable Direct Port Access via URL option on the Device Services page to enable direct port access for a KVM/serial port connect to the KSX II. See *Enabling Direct Port Access via URL* (on page 142).

▶ **To configure direct port access:**

1. Choose Device Settings > Device Services. The Device Service Settings page opens.

2. Type the IP address and ports used for SSH and Telnet in the appropriate fields for each serial target.

   Note that leaving all three fields blank will disable direct port access for the serial target. To enable direct port access, you must do one of the following:

   ▪ Enable global Telnet or SSH access.

   ▪ Input a valid IP address or TCP port in at least one of the three fields.

   Important: It is not recommended that more than one of these fields is populated.

   Below are examples of Telnet and IP:

   ▪ Direct Port access via IP alias address:

      Configure the IP alias address 192.168.1.59 for a serial target. Once this is done, connection to the target through Telnet can be done using "telnet 192.168.1.59".

   ▪ Direct Port access via Telnet port:

      Configure the Telnet TCP Port as "7770". Once this is done, connection to the target can be done using "telnet <KSX II device IP address> 7770".

   ▪ Direct Port Access via SSH Port:

> Configure the SSH TCP port as "7888". Once this is done, connection to the target can be done by using "ssh –l <login> <KSX II device IP address> -p 7888".

3. Click OK to save this information.

Direct Port Access

No.	Name	IP Address	SSH Port	Telnet Port
9	Serial Port 1			
10	Serial Port 2			
11	Serial Port 3			
12	Serial Port 4			
13	Serial Port 5			
14	Serial Port 6			
15	Serial Port 7			
16	Serial Port 8			

OK   Reset To Defaults   Cancel

Once you have created the direct port access, it can be connected in a client application such as PuTTY. Following is an example of how the direct port access information would appear in PuTTY. Note that PuTTY is not the only client application that can be used. It is used here for sample purposes only.

Note to CC-SG Users

Note to CC-SG Users

If you are using the KSX II in a CC-SG configuration, perform the installation steps, and when finished, consult the **CommandCenter Secure Gateway User Guide**, **Administrator Guide**, or **Deployment Guide** to proceed (all found on Raritan's website, www.raritan.com, under Support).

Note: The remainder of this help applies primarily to deploying the KSX II device(s) without the integration functionality of CC-SG.

Remote Authentication

Note to CC-SG Users

When the KSX II is controlled by CommandCenter Secure Gateway, CC-SG authenticates users and groups, except for local users requiring Local port access. When CC-SG is controlling the KSX II, Local port users will be authenticated against the local user database or the remote authentication server (LDAP/LDAPS or RADIUS) configured on the KSX II. They will not be authenticated against the CC-SG user database.

For additional information about CC-SG authentication, see the CommandCenter Secure Gateway User Guide, Administrator Guide, or Deployment Guide, which can be downloaded from the Support section of the *Raritan website http://www.raritan.com*.

Supported Protocols

To simplify management of usernames and passwords, the KSX II provides the ability to forward authentication requests to an external authentication server. Two external authentication protocols are supported: LDAP/LDAPS and RADIUS.

Note on Microsoft Active Directory

Microsoft® Active Directory® uses the LDAP/LDAPS protocol natively, and can function as an LDAP/LDAPS server and authentication source for the KSX II. If it has the IAS (Internet Authorization Server) component, a Microsoft Active Directory server can also serve as a RADIUS authentication source.

Create User Groups and Users

As part of the initial configuration, you must define user groups and users in order for users to access the KSX II.

The KSX II uses system-supplied default user groups and allows you to create groups and specify the appropriate permissions to suit your needs.

User names and passwords are required to gain access to the KSX II. This information is used to authenticate users attempting to access your KSX II.

See **User Management** for details on adding and editing user groups and users.

Step 5 (Optional): Configure Keyboard Language

Note: This step is not required if you are using the US/International language keyboard.

If you are using a non-US language, the keyboard has to be configured for the appropriate language. In addition, the keyboard language for the client machine and the KVM target servers has to match.

Consult the documentation for your operating system for additional information about changing the keyboard layout.

Changing the Keyboard Layout Code (Sun Targets)

Use this procedure if you are using a DCIM-SUSB and would like the keyboard layout changed to another language.

▶ **To change the keyboard layout code (DCIM-SUSB only):**

1. Open a Text Editor window on the Sun™ workstation.

2. Check that the Num Lock key is active and press the left Ctrl key and the Del key on your keyboard. The Caps Lock light starts to blink, indicating that the CIM is in Layout Code Change mode. The text window displays: `Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX).`

3. Type the layout code desired (for example, *31* for the Japanese keyboard).

4. Press Enter.

5. Shut down the device and power on once again. The DCIM-SUSB performs a reset (power cycle).

6. Verify that the characters are correct.

Chapter 3   Working with Target Servers

In This Chapter

Interfaces

There are several interfaces in the KSX II providing you with easy access any time, anywhere. The following table identifies these interfaces and their use of target server access and administration locally and remotely:

	Local		Remote	
User interface	Access	Admin	Access	Admin
KSX II Local Console	✓	✓		
KSX II Remote Console			✓	✓
Virtual KVM Client (VKC)			✓	
Active KVM Client (AKC)			✓	✓
Multi-Platform Client (MPC)			✓	✓
Raritan Serial Console (RSC)			✓	
Command Line Interface (CLI)	✓	✓	✓	✓

The following sections of the user guide contain information about using specific interfaces to connect to the KSX II and manage targets:

- *KSX II Local Console Interface: KSX II Devices* (see "*KSX II Local Console: KSX II Devices*" on page 39)

- *KSX II Remote Console Interface* (on page 40)

- *Virtual KVM Client (VKC)* (on page 53)

- *Active KVM Client (AKC)* (on page 80)

- *Multi-Platform Client (MPC)* (on page 82)

- *Raritan Serial Console (RSC)* (on page 83)

- *Command Line Interface (CLI)* (on page 225)

KSX II Local Console: KSX II Devices

When you are located at the server rack, the KSX II provides standard KVM management and administration via the KSX II Local Console. The KSX II Local Console provides a direct KVM (analog) connection to your connected servers; the performance is exactly as if you were directly connected to the server's keyboard, mouse, and video ports. Additionally, the KSX II provides terminal emulation when accessing serial targets.

There are many similarities among the KSX II Local Console and the KSX II Remote Console graphical user interfaces. Where there are differences, they are noted in the help.

KSX II Remote Console Interface

The KSX II Remote Console is a browser-based graphical user interface that allows you to log in to KVM target servers and serial targets connected to the KSX II and to remotely administer the KSX II.

The KSX II Remote Console provides a digital connection to your connected KVM target servers. When you log into a KVM target server using the KSX II Remote Console, a Virtual KVM Client window opens.

There are many similarities among the KSX II Local Console and the KSX II Remote Console graphical user interfaces, and where there are differences, they are noted in the user manual. The following options are available in the KSX II Remote Console but not the KSX II Local Console:

- Virtual Media
- Favorites
- Backup/Restore
- Firmware Upgrade
- Upgrade Report
- SSL Certificates

Note: If you are using Internet Explorer® 7, you may run into permission issues when trying to connect to a target server. To avoid this, do the following:

1. In Internet Explorer, click Tools > Internet Options to open the Internet Options dialog.

2. In the "Temporary Internet files" section, click the Settings button. The Settings dialog opens.

3. In the "Check for newer versions of stored pages" section, select Automatically.

4. Click OK to apply the settings.

Launching the KSX II Remote Console

Important: Regardless of the browser used, you must allow pop-ups from the device's IP address to launch the KSX II Remote Console.

Depending on your browser and security settings, you may see various security and certificate warnings. It is necessary to accept these warnings to launch the KSX II Remote Console.

You can reduce the number of warning messages during subsequent log ins by checking the following options on the security and certificate warning messages:

- In the future, do not show this warning.

- Always trust content from this publisher.

▶ **To launch the KSX II Remote Console:**

1. Log in to any workstation with network connectivity to your KSX II and Java Runtime Environment® installed (JRE® is available on the *Java website http://java.sun.com/*).

2. Launch a supported web browser such as Internet Explorer® or Firefox®.

3. Type the following URL: *http://IP-ADDRESS*, where IP-ADDRESS is the IP address assigned to your KSX II. You can also use https, the DNS name of the KSX II assigned by the administrator (provided that a DNS server has been configured), or just simply type the IP address in the browser (KSX II always redirects the IP address from HTTP to HTTPS.) The Login page opens.

4. Type your user name and password. If this is the first time logging in, log in with the factory default user name (admin) and password (raritan, all lower case). You will be prompted to change the default password.   Click Login.

Note: If your administrator requires you read and/or accept a security agreement in order to access the device, a security banner will be displayed after you have entered your login credentials and clicked Login.

See **Virtual KVM Client** (see "**Virtual KVM Client (VKC)**" on page 53) for information on the KSX II functions available via the Remote Console.

Interface and Navigation

KSX II Console Layout

Both the KSX II Remote Console and the KSX II Local Console interfaces provide an HTML (web-based) interface for configuration and administration, as well as target server list and selection. The options are organized into various tabs.

After successful login, the Port Access page opens listing all ports along with their status and availability. Three tabs are provided on the page allowing you to view by port, view by group or view by search. You can sort by Port Number, Port Name, Status (Up and Down), and Availability (Idle, Connected, Busy, Unavailable, and Connecting) by clicking on the column heading. See Port Access Page for more information.

Left Panel

The left panel of the KSX II interface contains the following information. Note that some information is conditional and will only be displayed if you are a certain of user, are using certain features, and so on. This conditional information is noted here.

Information	Description	When displayed?
Time & Session	The date and time the current session started.	Always
User	Username	Always
State	The current state of the application, either idle or active. If idle, the application tracks and displays the time the session has been idle.	Always
Your IP	The IP address used to access the KSX II.	Always
Last Login	The last login date and time.	Always
Under CC-SG Management	The IP address of the CC-SG device managing the KSX II.	When the KSX II is being managed by CC-SG.
Device Information	Information specific to the KSX II you are using.	Always
Device Name	Name assigned to the device.	Always
IP Address	The IP address of the KSX II. If IPv6 is enabled, the IPv6 address will also be listed.	Always
Firmware	Current version of firmware.	Always
Device Model	Model of the KSX II	Always
Network	The name assigned to the current network.	Always
Port States	The statuses of the ports being used by the KSX II.	Always

Information	Description	When displayed?
Connected Users	The users, identified by their username and IP address, who are currently connected to the KSX II.	Always
Online Help - User Guide	Links to online help.	Always
Favorite Devices	See **Managing Favorites** (on page 48).	Always
FIPS Mode	FIPS Mode: EnabledSSL Certificate: FIPS Mode Compliant	When FIPS is enabled.

Port Access Page

After successfully logging on to the KSX II Remote Console, the Port Access page appears. This page lists all of the KSX II ports, the connected KVM target servers, and their status and availability. The Port Access page provides access to the KVM target servers connected to the KSX II. KVM target servers are servers that you want to control through the KSX II device. They are connected to the KSX II ports at the back of the device.

Note: For each connection to a KVM target server, a new Virtual KVM Client page is opened.

Also displayed on the Port Access page are blade chassis that have been configured in the KSX II. The blade chassis is displayed in an expandable, hierarchical list on the Port Access page, with the blade chassis at the root of the hierarchy and the individual blades labeled and displayed below the root. Use the Expand Arrow icon next to the root chassis to display the individual blades.

Note: To view the blade chassis in a hierarchal order, blade-chassis subtypes must be configured for the blade server chassis.

By default, the View by Port tab will be displayed on the Port Access page. The View by Group tab displays port groups and can be expandable to display ports that are assigned to the port group. The View by Search tab allows you to search by port name. The search feature supports the use of an asterisk (*) as a wildcard, and full and partial names.

► **To use the Port Access page:**

1. From the KSX II Remote Console, click the Port Access tab. The Port Access page opens.

2. The KVM target servers are initially sorted by Port Number. You can change the display to sort on any of the columns.

   ▪ Port Number - Numbered from 1 to the total number of ports available for the KSX II device.

   ▪ Port Name - The name of the KSX II port. Initially, this is set to Dominion-KSX2-Port# but you can change the name to something more descriptive. When you click a Port Name link, the Port Action Menu appears.

   Note: Do not use apostrophes for the Port (CIM) Name.

   ▪ Status - The status for standard servers is either up or down.

   ▪ Type - The type of server or CIM. For blade chassis, the type can be Blade Chassis, Blade, BladeChassisAdmin, and BladeChassisURL.

▪ Availability - The Availability can be Idle, Connected, Busy, or Unavailable. Blade servers will have an availability of either shared or exclusive when a connection to that blade is in place.

3. Click View by Port, View by Group   or View by Search to switch between views.

4. Click the Port Name of the target server you want to access. The Port Action Menu appears. See **Port Action Menu** (on page 46) for details on available menu options.

5. Choose the desired menu command from the Port Action Menu.

▶ **To change the display sort order:**

• Click the column heading by which you want to sort. The list of KVM target servers is sorted by that column.

Port Action Menu

When you click a Port Name in the Port Access list, the Port Action menu appears. Choose the desired menu option for that port to execute it. Note that only currently available options, depending on the port's status and availability, will be listed in the Port Action menu:

• Connect - Creates a new connection to the target server. For the KSX II Remote Console, a new *Virtual KVM Client* (see "*Virtual KVM Client (VKC)*" on page 53) page appears. For the KSX II Local Console, the display switches to the target server and switches away from the local user interface. On the local port, the KSX II Local Console interface must be visible in order to perform the switch. Hot key switching is also available from the local port.

Note: This option is not available from the KSX II Remote Console for an available port if all connections are busy.

• Switch From - Switches from an existing connection to the selected port (KVM target server). This menu item is available only for KVM targets. This option is visible only when a Virtual KVM Client is opened.

Note: This menu item is not available on the KSX II Local Console.

• Disconnect - Disconnects this port and closes the Virtual KVM Client page for this target server. This menu item is available only when the port status is up and connected, or up and busy.

Note: This menu item is not available on the KSX II Local Console. The only way to disconnect from the switched target in the Local Console is to use the hot key.

- Power On - Powers on the target server through the associated outlet. This option is visible only when there are one or more power associations to the target.

- Power Off - Powers off the target server through the associated outlets. This option is visible only when there are one or more power associations to the target, when the target power is on (port status is up), and when user has permission to operate this service.

- Power Cycle - Power cycles the target server through the associated outlets. This option is visible only when there are one or more power associations to the target, and when the user has permission to operate this service.

Managing Favorites

A Favorites feature is provided so you can organize and quickly access the devices you use frequently. The Favorite Devices section is located in the lower left side (sidebar) of the Port Access page and provides the ability to:

- Create and manage a list of favorite devices
- Quickly access frequently-used devices
- List your favorites either by Device Name, IP Address, or DNS hostname
- Discover KSX II devices on its subnet (before and after login)
- Retrieve discovered KSX II devices from the connected KX device (after login)

▶ **To access a favorite KSX II device:**

- Click the device name (listed beneath Favorite Devices). A new browser opens to that device.

▶ **To display favorites by name:**

- Click Display by Name.

▶ **To display favorites by IP Address:**

- Click Display by IP.

▶ **To display favorites by the host name:**

- Click Display by Host Name.
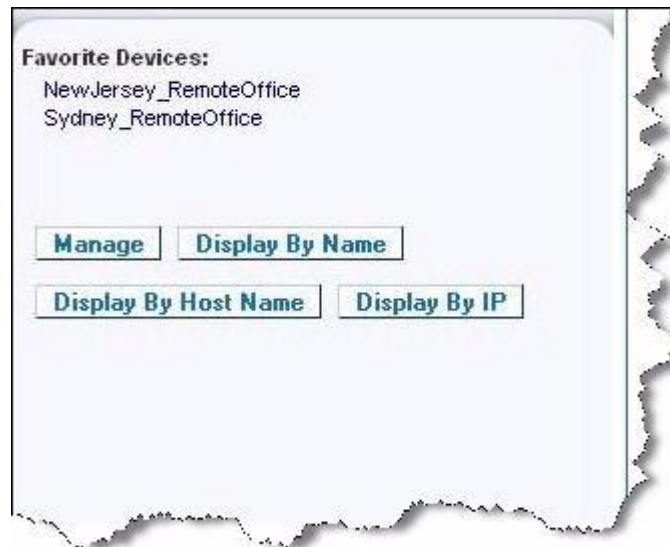
Note: Both IPv4 and IPv6 addresses are supported.

Manage Favorites Page

▶ **To open the Manage Favorites page:**

- Click the Manage button in the left panel. The Manage Favorites page appears and contains the following:

Use:	To:
Favorites List	Manage your list of favorite devices.
Discover Devices - Local Subnet	Discover Raritan devices on the client PC's local subnet.
Discover Devices - KSX II Subnet	Discover the Raritan devices on the KSX II device subnet.
Add New Device to Favorites	Add, edit, and delete devices from your list of Favorites.

Favorites List Page

From the Favorites List page, you can add, edit, and delete devices from your list of favorites.

▶ **To open the Favorites List page:**

- Choose Manage > Favorites List. The Favorites List page opens.

Discovering Devices on the Local Subnet

This option discovers the devices on your local subnet, which is the subnet where the KSX II Remote Console is running. These devices can be accessed directly from this page or you can add them to your list of favorites. See **Favorites List Page** (on page 49).

▶ **To discover devices on the local subnet:**

1. Choose Manage > Discover Devices - Local Subnet. The Discover Devices - Local Subnet page appears.

2. Choose the appropriate discovery port:

   ▪ To use the default discovery port, select the Use Default Port 5000 checkbox.

   ▪ To use a different discovery port:

   a. Deselect the Use Default Port 5000 checkbox.

   b. Type the port number in the Discover on Port field.

    c.   Click Save.

3.   Click Refresh. The list of devices on the local subnet is refreshed.

▶   **To add devices to your Favorites List:**

1.   Select the checkbox next to the device name/IP address.

2.   Click Add.

Tip: Use the Select All and Deselect All buttons to quickly select all (or deselect all) devices in the remote console subnet.

▶   **To access a discovered device:**

●   Click the device name or IP address for that device. A new browser opens to that device.

Note: Both IPv4 and IPv6 addresses are supported.

Discovering Devices on the KSX II Subnet

This option discovers devices on the device subnet, which is the subnet of the KSX II device IP address itself. You can access these devices directly from this the Subnet page or add them to your list of favorites. See **Favorites List Page** (on page 49).

This feature allows multiple KSX II devices to interoperate and scale automatically. The KSX II Remote Console automatically discovers the KSX II devices, and any other Raritan device, in the subnet of the KSX II.

▶   **To discover devices on the device subnet:**

1.   Choose Manage > Discover Devices - KSX II Subnet. The Discover Devices - KSX II Subnet page appears.

2.   Click Refresh. The list of devices on the local subnet is refreshed.

▶   **To add devices to your Favorites List:**

1.   Select the checkbox next to the device name/IP address.

2.   Click Add.

Tip: Use the Select All and Deselect All buttons to quickly select all (or deselect all) devices in the KSX II device subnet.

▶   **To access a discovered device:**

●   Click the device name or IP address for that device. A new browser opens to that device.

Note: Both IPv4 and IPv6 addresses are supported.

Adding, Deleting and Editing Favorites

▶ **To add a device to your favorites list:**

1. Choose Manage > Add New Device to Favorites. The Add New Favorite page appears.

2. Type a meaningful description.

3. Type the IP Address/Host Name for the device.

4. Change the discovery Port (if necessary).

5. Select the Product Type.

6. Click OK. The device is added to your list of favorites.

▶ **To edit a favorite:**

1. From the Favorites List page, select the checkbox next to the appropriate KSX II device.

2. Click the Edit button. The Edit page appears.

3. Update the fields as necessary:

    ▪ Description

    ▪ IP Address/Host Name - Type the IP address of the KSX II device

    ▪ Port (if necessary)

    ▪ Product Type

4. Click OK.

▶ **To delete a favorite:**

Important: Exercise caution in the removal of favorites. You are not prompted to confirm their deletion.

1. Select the checkbox next to the appropriate KSX II device.

2. Click the Delete button. The favorite is removed from your list of favorites.

Note: Both IPv4 and IPv6 addresses are supported.

Logging Out

▶ **To quit the KSX II Remote Console:**

• Click Logout in the upper right-hand corner of the page.

Note: Logging out also closes any open Virtual KVM Client and serial client sessions.

Proxy Server Configuration for use with KSX II, MPC, VKC and AKC

When the use of a Proxy Server is required, a SOCKS proxy must also be provided and configured on the remote client PC.

Note: If the installed proxy server is only capable of the HTTP proxy protocol, you will not be able to connect.

▶ **To configure the SOCKS proxy:**

1. On the client, select Control Panel > Internet Options.

a. On the Connections tab, click 'LAN settings'. The Local Area Network (LAN) Settings dialog opens.

b. Select 'Use a proxy server for your LAN'.

c. Click Advanced. The Proxy Settings dialog opens.

d. Configure the proxy servers for all protocols. IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

Note: The default port for a SOCKS proxy (1080) is different from HTTP proxy (3128).

2. Click OK at each dialog to apply the settings.

3. Next, configure the proxies for Java™ applets by selecting Control Panel > Java.

e. On the General tab, click Network Settings. The Network Settings dialog opens.

f. Select Use Proxy Server.

g. Click Advanced. The Advanced Network Settings dialog opens.

h. Configure the proxy servers for all protocols.   IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

Note: The default port for a SOCKS proxy (1080) is different from HTTP proxy (3128).

4. If you are using standalone MPC, you must also do the following:

i. Open the start.bat file in MPC directory with a text editor.

j. Insert the following parameters to the command line. Add them before "-classpath": -DsocksProxyHost=<socks proxy ip addr> -DsocksProxyPort=<socks proxy port>

The parameters should look as follows:

```
start javaw -Xmn128M -Xmx512M -XX:MaxHeapFreeRatio=70
-XX:MinHeapFreeRatio=50 -Dsun.java2d.noddraw=true
-DsocksProxyHost=192.168.99.99 -DsocksProxyPort=1080
-classpath .\sdeploy.jar;.\sFoxtrot.jar;.\jaws.jar;.\sMpc.jar
com.raritan.rrc.ui.RRCApplication %1
```

Virtual KVM Client (VKC)

Please note this client is used by various Raritan products. As such, references to other products may appear in this section of help since they are shared between products.

Overview

Whenever you access a target server using the Remote Console, a Virtual KVM Client (VKC) window opens. There is one Virtual KVM Client for each target server connected. These windows can be accessed via the Windows® task bar.

Virtual KVM Client windows can be minimized, maximized, and moved around your computer desktop.

Note: Refreshing your HTML browser will close the Virtual KVM Client connection, so exercise caution.

Note: If you are using Firefox 3.0.3, you may experience problems launching the application. If this occurs, clear the browser cache and launch the application again.

Connecting to a KVM Target Server

▶ **To connect to a KVM target server:**

1. From the KSX II Remote Console, click the Port Access tab to open it. The Port Access page opens.

2. Click the Port Name of the target you want to access. The Port Action menu appears.

3. Click Connect. A *Virtual KVM Client* (see "*Virtual KVM Client (VKC)*" on page 53) window opens to the target server connected to that port.

Toolbar

Note: The KX II-101 VKC interface is different from the other Dominion KX products. See VKC Toolbar for the KX II-101.

Button	Button Name	Description
	Connection Properties	Opens the Modify Connection Properties dialog from which you can manually adjust bandwidth options (such as connection speed, color depth, and so forth).
	Video Settings	Opens the Video Settings dialog, allowing you to manually adjust video conversion parameters.
	Color Calibration	Adjusts color settings to reduce excess color noise. Same as choosing Video > Color Calibrate.
	Target Screenshot	Click to take a screenshot of the target server and save it to a file of your choosing.
	Synchronize Mouse	In dual-mouse mode, forces realignment of the target server mouse pointer with the mouse pointer.
	Refresh Screen	Forces a refresh of the video screen.
	Auto-sense Video Settings	Forces a refresh of the video settings (resolution, refresh rate).
	Smart Card	Opens a dialog that allows you to select from a list of smart card readers connected to a client PC. *Note: This function is only available on the KSX II 2.3.0 or later, and the KX II 2.1.10 or later.*
	Send Ctrl+Alt+Del	Sends a Ctrl+Alt+Del hot key combination to the target server.
	Single Cursor Mode	Starts Single Cursor mode in which the local mouse pointer no longer appears onscreen. Press Ctrl+Alt+O to exit this mode. Alternatively, choose Single/Double Cursor from the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.

Button	Button Name	Description
	Full Screen Mode	Maximizes the screen real estate to view the target server desktop.
	Scaling	Increases or reduces the target video size so you can view the entire contents of the target server window without using the scroll bar.

Switching Between KVM Target Servers

With the KSX II, you can access several KVM target servers. The KSX II provides the ability to switch from one target server to another.

Note: This feature is available in the KSX II Remote Console only.

▶ **To switch between KVM target servers:**

1. While already using a target server, access the KSX II Port Access page.

2. Click the port name of the target you want to access. The Port Action menu appears.

3. Choose Switch From in the Port Action menu. The Virtual KVM Client window switches to the new target server you selected.

Power Controlling a Target Server

Note: These features are available only when you have made power associations.

▶ **To power cycle a KVM target server:**

1. From the KSX II Remote Console, click the Port Access tab. The Port Access page opens.

2. Click the Port Name of the appropriate target server. The Port Action menu appears.

3. Choose Power Cycle. A confirmation message appears.

▶ **To power on a target server:**

1. From the KSX II Remote Console, click the Port Access tab. The Port Access page opens.

2. Click the port name of the appropriate target server. The Port Action menu appears.

3. Choose Power On. A confirmation message appears.

► **To power off a target server:**

1. From the KSX II Remote Console, click the Port Access tab to open it. The Port Access page opens.

2. Click the port name of the appropriate target server. The Port Action menu appears.

3. Choose Power Off. A confirmation message appears.

Disconnecting KVM Target Servers

Note: This item is not available on the KSX II Local Console. The only way to disconnect from the switched target in the Local Console is to use the hot key.

► **To disconnect a target server:**

1. Click the port name of the target you want to disconnect. The Port Action menu appears.

2. Choose Disconnect.

Tip: You can also close the Virtual KVM Client window by selecting Connection > Exit from the Virtual KVM menu.

Choosing USB Profiles

When you connect to a KVM target server for the first time, as described in **Connecting to a KVM Target Server** (on page 53), the preferred USB profile for the port is automatically used. If you have connected to the target server previously using a different profile, the USB profile from the last connection is used. You are alerted to the use of a profile other than the preferred profile by a warning similar to the following:
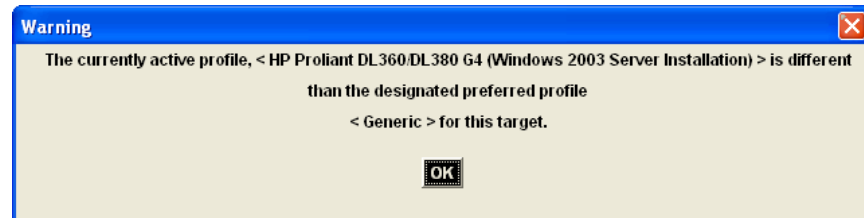
After you have connected to a target server, you can change the USB profile as necessary. By default, the profiles that appear under the USB Profile menu in the VKC are those that you are most likely to use. These profiles have been preselected by the administrator for use with the connected target server, based on your operational requirements. However, all profiles are available to be selected via the Other Profiles option on the USB Profile menu.

▶ **To choose a USB profile:**

1. Connect to a KVM target server as described in **Connecting to a KVM Target Server** (on page 53).

2. In VKC, choose a USB profile from the USB Profile menu.

   The name of the profile indicates the operating system or server with which it should be used. See **USB Profiles** (on page 104) for details on USB profiles.

Connection Properties

The dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints. The devices optimize KVM output not only for LAN use, but also for WAN use. These devices can also control color depth and limit video output, offering an optimal balance between video quality and system responsiveness for any bandwidth.

The parameters in the Properties dialog can be optimized to suit your needs for different operating environments. Connection properties are saved across subsequent connections to generation 2 devices once they are set and saved.

Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See VKC Toolbar for the KX II-101 for additional information.

▶ **To set the connection properties:**

1. Choose Connection > Properties or click the Connection Properties button in the toolbar. The Properties dialog appears.
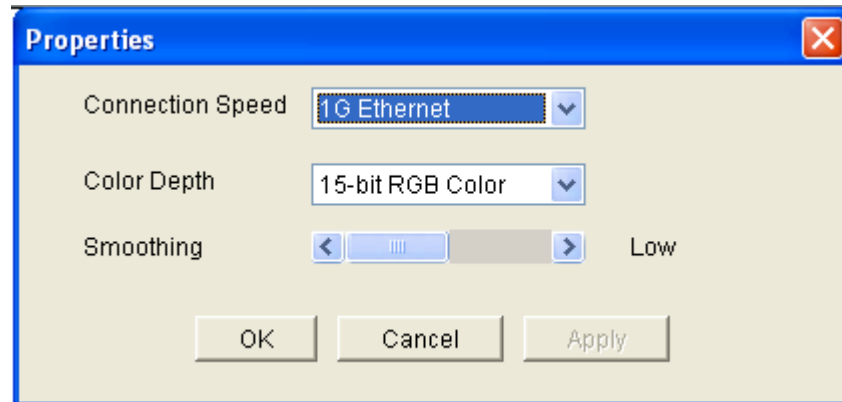
Note: KX II-101 does not support 1G Ethernet.

Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See VKC Toolbar for the KX II-101 for additional information.

2. Choose the Connection Speed from the drop-down list. The device can automatically detect available bandwidth and not limit bandwidth use. However, you can also adjust this usage according to bandwidth limitations.

   ▪ Auto
   ▪ 1G Ethernet

- 100 Mb Ethernet
- 10 Mb Ethernet
- 1.5 Mb (MAX DSL/T1)
- 1 Mb (Fast DSL/T1)
- 512 Kb (Medium DSL/T1)
- 384 Kb (Slow DSL/T1)
- 256 Kb (Cable)
- 128 Kb (Dual ISDN)
- 56 kb (ISP Modem)
- 33 kb (Fast Modem)
- 24 kb (Slow Modem)

Note that these settings are an optimization for specific conditions rather than an exact speed. The client and server always attempt to deliver video as quickly as possible on the network regardless of the current network speed and encoding setting. But the system will be most responsive when the settings match the real world environment.

3. Choose the Color Depth from the drop-down list. The device can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidths.

- 15-bit RGB Color
- 8-bit RGB Color
- 4-bit Color
- 4-bit Gray
- 3-bit Gray
- 2-bit Gray
- Black and White

Important: For most administrative tasks (server monitoring, reconfiguring, and so on), the full 24-bit or 32-bit color spectrum made available by most modern video graphics cards is not necessary. Attempting to transmit such high color depths wastes network bandwidth.

4. Use the slider to select the desired level of Smoothing (15-bit color mode only). The level of smoothing determines how aggressively to blend screen regions with small color variation into a single smooth color. Smoothing improves the appearance of target video by reducing displayed video noise.

5. Click OK to set these properties.

Connection Information

▶ **To obtain information about your Virtual KVM Client connection:**

- Choose Connection > Connection Info. The Connection Info window opens.

The following information is displayed about the current connection:

- Device Name - The name of the device.
- IP Address - The IP address of the device.
- Port - The KVM communication TCP/IP port used to access the target device.
- Data In/Second - Data rate in.
- Data Out/Second - Data rate out.
- Connect Time - The duration of the connect time.
- FPS - The frames per second transmitted for video.
- Horizontal Resolution - The screen resolution horizontally.
- Vertical Resolution - The screen resolution vertically.
- Refresh Rate - How often the screen is refreshed.
- Protocol Version - RFB Protocol version.

▶ **To copy this information:**

- Click Copy to Clipboard. The information is available to be pasted into the program of your choice.

Keyboard Options

Keyboard Macros

Keyboard macros ensure that keystroke combinations intended for the target server are sent to and interpreted only by the target server. Otherwise, they might be interpreted by the computer on which the Virtual KVM Client is running (your client PC).

Macros are stored on the client PC and are PC-specific. Therefore, if you use another PC, you will not see your macros. In addition, if another person uses your PC and logs in under a different name, that user will see your macros since they are computer-wide.

Keyboard macros created in the Virtual KVM Client are available in MPC and vice versa. However, keyboard macros created in AKC cannot be used in VKC or MPC, and vice versa.

Building a Keyboard Macro

▶ **To build a macro:**

1. Click Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.

2. Click Add. The Add Keyboard Macro dialog appears.

3. Type a name for the macro in the Keyboard Macro Name field. This name will appear in the Keyboard menu after it is created.

4. From the Hot-Key Combination field, select a keyboard combination from the drop-down list. This allows you to execute the macro with a predefined keystroke. **Optional**

5. In the Keys to Press drop-down list, select each key you would like to use to emulate the keystrokes that will be used to perform the command. Select the keys in the order by which they are to be pressed. After each selection, select Add Key. As each key is selected, it will appear in the Macro Sequence field and a Release Key command will automatically be added after each selection.

6. To use the Send Text to Target function for the macro, click the Construct Macro from Text button.

7. For example, create a macro to close a window by selecting Left Ctrl + Esc. This will appear in the Macro Sequence box as follows:

    Press Left Ctrl

    Release Left Ctrl

    Press Esc

    Release Esc

8. Review the Macro Sequence field to be sure the macro sequence is defined correctly.

    a. To remove a step in the sequence, select it and click Remove.

    b. To change the order of steps in the sequence, click the step and then click the up or down arrow buttons to reorder them as needed.

9. Click OK to save the macro. Click Clear to clear all field and start over. When you click OK, the Keyboard Macros dialog appears and lists the new keyboard macro.

10. Click Close to close the Keyboard Macros dialog. The macro will now appear on the Keyboard menu in the application. Select the new macro on the menu to run it or use the keystrokes you assigned to the macro.
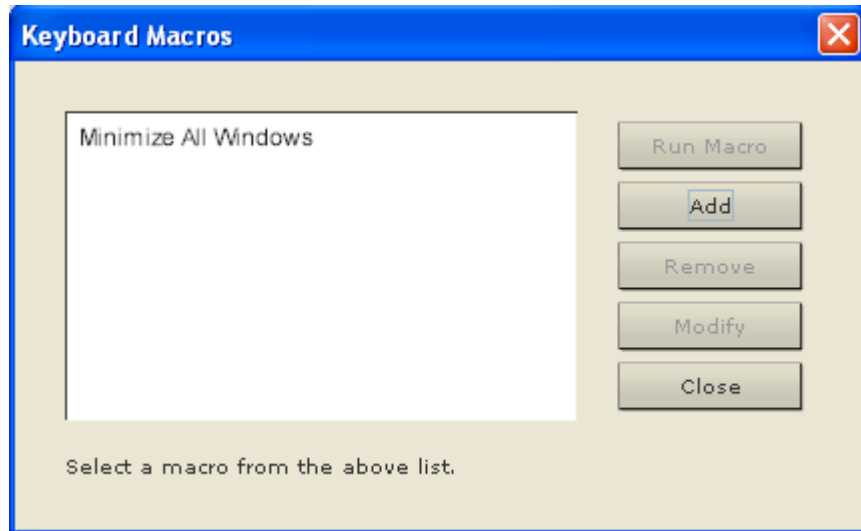
Running a Keyboard Macro

Once you have created a keyboard macro, execute it using the keyboard macro you assigned to it or by choosing it from the Keyboard menu.

Run a Macro from the Menu Bar

When you create a macro, it appears under the Keyboard menu. Execute the keyboard macro by clicking on it in the Keyboard menu.

Run a Macro Using a Keyboard Combination

If you assigned a keyboard combination to a macro when building it, you can execute the macro by pressing its assigned keystrokes. For example, press the keys Ctrl+Alt+0 simultaneously to minimize all windows on a Windows target server.

Modifying and Removing Keyboard Macros

▶ **To modify a macro:**

1. Choose Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.

2. Choose the macro from among those listed.

3. Click Modify. The Add/Edit Macro dialog appears.

4. Make your changes.

5. Click OK.

▶ **To remove a macro:**

1. Choose Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.

2. Choose the macro from among those listed.

3. Click Remove. The macro is deleted.

Hot-key combinations that coincide with blade chassis switching key sequences will not be sent to blades housed in those chassis.

Setting CIM Keyboard/Mouse Options

▶ **To access the DCIM-USBG2 setup menu:**

1. Put the mouse focus on a window such as Note Pad (Windows® operating system) or an equivalent.

2. Select Set CIM Keyboard/Mouse options. This is the equivalent of sending the Left-Control and Num Lock to the target. The CIM setup menu options are then displayed.

3. Set the language and mouse settings.

4. Exit the menu to return to normal CIM functionality.

Video Properties

Refresh Screen

The Refresh Screen command forces a refresh of the video screen. Video settings can be refreshed automatically in several ways:

- The Refresh Screen command forces a refresh of the video screen.

- The Auto-sense Video Settings command automatically detects the target server's video settings.

- The Calibrate Color command calibrates the video to enhance the colors being displayed.

In addition, you can manually adjust the settings using the Video Settings command.

Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See VKC Toolbar for the KX II-101 for additional information.

▶ **To refresh the video settings, do one of the following:**

- Choose Video > Refresh Screen or click the Refresh Screen button in the toolbar.

Auto-Sense Video Settings

The Auto-sense Video Settings command forces a re-sensing of the video settings (resolution, refresh rate) and redraws the video screen.

Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See VKC Toolbar for the KX II-101 for additional information.

▶ **To automatically detect the video settings, do the following:**

- Choose Video > Auto-sense Video Settings or click the Auto-Sense Video Settings button ⬚ in the toolbar. A message stating that the auto adjustment is in progress appears.

Calibrating Color

Use the Calibrate Color command to optimize the color levels (hue, brightness, saturation) of the transmitted video images. The color settings are on a target server-basis.

Note: The Calibrate Color command applies to the current connection only.

Note: The KX II-101 does support color calibration.

▶ **To calibrate the color, do the following:**

- Choose Video > Calibrate Color or click the Calibrate Color button ⬚ in the toolbar. The target device screen updates its color calibration.

Adjusting Video Settings

Use the Video Settings command to manually adjust the video settings.

▶ **To change the video settings:**

1. Choose Video > Video Settings or click the Video Settings button ⬚ in the toolbar to open the Video Settings dialog.

2. Adjust the following settings as required. As you adjust the settings the effects are immediately visible:

   a. Noise Filter

The device can filter out the electrical interference of video output from graphics cards. This feature optimizes picture quality and reduces bandwidth. Higher settings transmit variant pixels only if a large color variation exists in comparison to the neighboring pixels. However, setting the threshold too high can result in the unintentional filtering of desired screen changes.
Lower settings transmit most pixel changes. Setting this threshold too low can result in higher bandwidth use.

b. PLL Settings

Clock - Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended. Under most circumstances this setting should not be changed because the autodetect is usually quite accurate.

Phase - Phase values range from 0 to 31 and will wrap around. Stop at the phase value that produces the best video image for the active target server.

c. Brightness: Use this setting to adjust the brightness of the target server display.

d. Brightness Red - Controls the brightness of the target server display for the red signal.

e. Brightness Green - Controls the brightness of the green signal.

f. Brightness Blue - Controls the brightness of the blue signal.

g. Contrast Red - Controls the red signal contrast.

h. Contrast Green - Controls the green signal.

i. Contrast Blue - Controls the blue signal.

If the video image looks extremely blurry or unfocused, the settings for clock and phase can be adjusted until a better image appears on the active target server.

Warning: Exercise caution when changing the Clock and Phase settings. Doing so may result in lost or distorted video and you may not be able to return to the previous state. Contact Raritan Technical Support before making any changes.

j. Horizontal Offset - Controls the horizontal positioning of the target server display on your monitor.

k. Vertical Offset - Controls the vertical positioning of the target server display on your monitor.

3. Select Automatic Color Calibration to enable this feature.

4. Select the video sensing mode:

- Best possible video mode

  The device will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.

- Quick sense video mode

  With this option, the device will use a quick video Auto Sense in order to show the target's video sooner. This option is especially useful for entering a target server's BIOS configuration right after a reboot.

5. Click OK to apply the settings and close the dialog. Click Apply to apply the settings without closing the dialog.

Note: Some Sun background screens, such as screens with very dark borders, may not center precisely on certain Sun servers. Use a different background or place a lighter colored icon in the upper left corner of the screen.
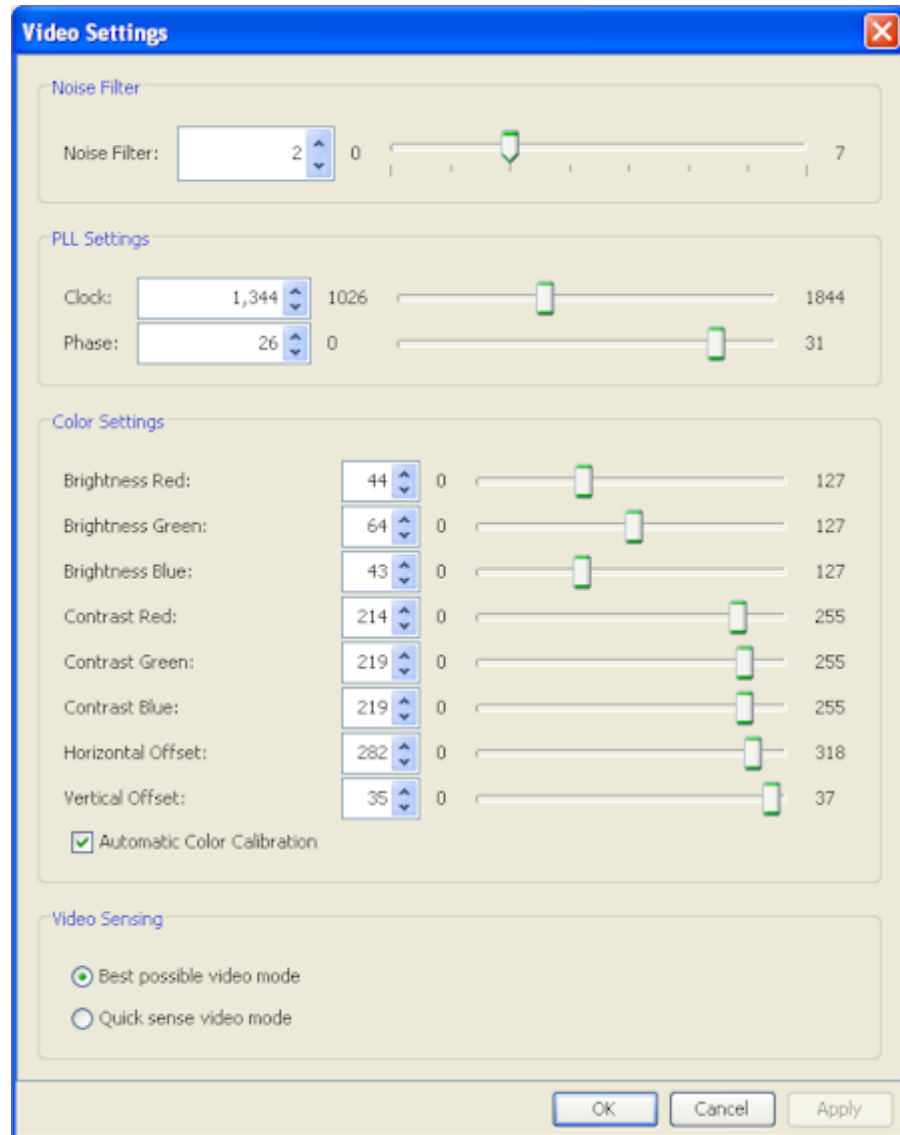
Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See VKC Toolbar for the KX II-101 for additional information.

Using Screenshot from Target

You are able to take a screenshot of a target server using the Screenshot from Target server command. You can then save this screenshot to a file location of your choosing as a bitmap, JPEG or PNG file.

Note: The Screenshot from Target function is not available for the KX II-101.

▶ **To take a screenshot of the target server:**

1. Select Video > Screenshot from Target or click the Screenshot from Target button ![icon] on the toolbar.

2. In the Save dialog, choose the location to save the file, name the file, and select a file format from the 'Files of type' drop-down.

3. Click Save to save the screenshot.

![Raritan logo]
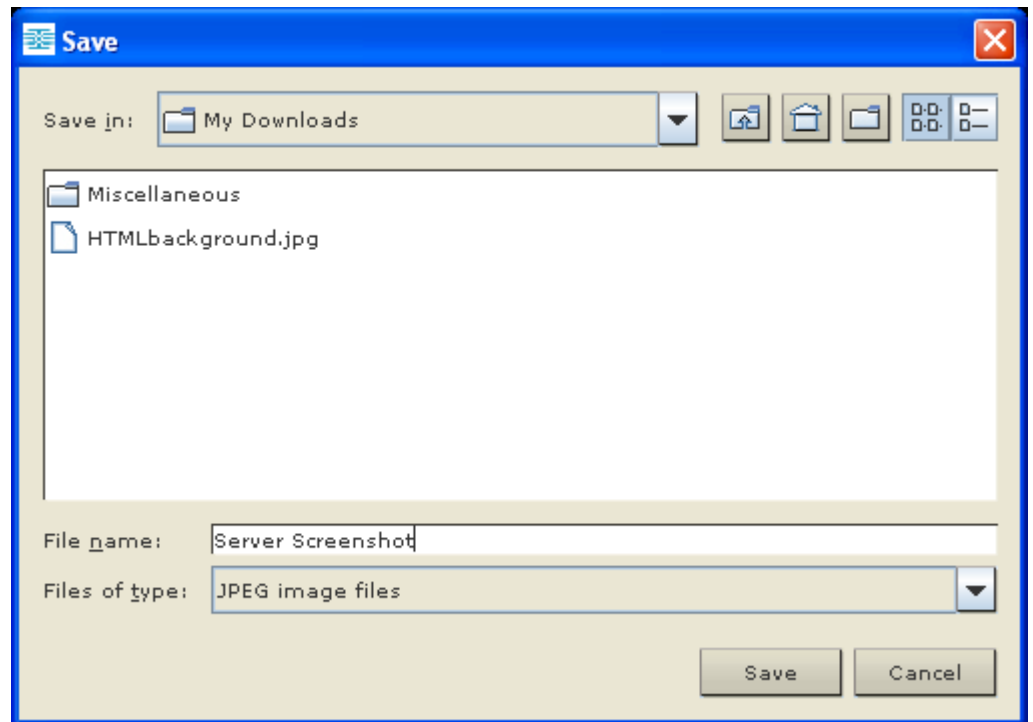
Changing the Maximum Refresh Rate

If the video card you are using on the target uses custom software and you are accessing the target through MPC or VKC, you may need to change the maximum refresh rate of the monitor in order for the refresh rate to take effect on the target.

▶ **To adjust the monitor refresh rate:**

1. In Windows®, select Display Properties > Settings > Advanced to open the Plug and Play dialog.

2. Click on the Monitor tab.

3. Set the 'Screen refresh rate'.

4. Click OK and then OK again to apply the setting.

Mouse Options

When controlling a target server, the Remote Console displays two mouse cursors: one belonging to your client workstation and the other belonging to the target server.

You can operate in either single mouse mode or dual mouse mode. When in dual mouse mode, and provided the option is properly configured, the mouse cursors will align.

When there are two mouse cursors, the device offers several mouse modes:

- Absolute (Mouse Synchronization)
- Intelligent (Mouse Mode)
- Standard (Mouse Mode)

Mouse Pointer Synchronization

When remotely viewing a target server that uses a mouse, you will see two mouse cursors: one belonging to your remote client workstation and the other belonging to the target server. When the mouse pointer lies within the Virtual KVM Client target server window, mouse movements and clicks are directly transmitted to the connected target server. While in motion, the client mouse pointer slightly leads the target mouse pointer due to mouse acceleration settings.

On fast LAN connections, you may want to disable the Virtual KVM Client mouse pointer and view only the target server's pointer. You can toggle between these two modes (single mouse and dual mouse).

Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See VKC Toolbar for the KX II-101 for additional information.

Mouse Synchronization Tips

Be sure to follow these steps when configuring mouse synchronization:

1. Verify that the selected video resolution and refresh rate are among those supported by the device. The Virtual KVM Client Connection Info dialog displays the actual values that the device is seeing.

2. Verify that the cable length is within the specified limits for the selected video resolution.

3. Verify that the mouse and video have been properly configured during the installation process.

4. Force an auto-sense by clicking the Virtual KVM Client auto-sense button.

5. If that does not improve the mouse synchronization (for Linux, UNIX, and Solaris KVM target servers):

    a. Open a terminal window.

    b. Enter the `xset mouse 1 1` command.

    c. Close the terminal window.

6. Click the "Virtual KVM Client mouse synchronization" button .

Additional Notes for Intelligent Mouse Mode

- Be sure that there are no icons or applications in the upper left section of the screen since that is where the synchronization routine takes place.

- Do not use an animated mouse.

- Disable active desktop on KVM target servers.

Synchronize Mouse

In dual mouse mode, the Synchronize Mouse command forces realignment of the target server mouse pointer with Virtual KVM Client mouse pointer.

▶ **To synchronize the mouse, do one of the following:**

- Choose Mouse > Synchronize Mouse or click the Synchronize Mouse button in the toolbar.

Note: This option is available only in Standard and Intelligent mouse modes.

Standard Mouse Mode

Standard Mouse mode uses a standard mouse synchronization algorithm using relative mouse positions. Standard Mouse mode requires that mouse acceleration is disabled and other mouse parameters are set correctly in order for the client and server mouse to stay synchronized.

▶ **To enter Standard Mouse mode:**

- Choose Mouse > Standard.

Intelligent Mouse Mode

In Intelligent Mouse mode, the device can detect the target mouse settings and synchronize the mouse cursors accordingly, allowing mouse acceleration on the target. Intelligent mouse mode the default for non-VM targets.

In this mode, the mouse cursor does a "dance" in the top left corner of the screen and calculates the acceleration. For this mode to work properly, certain conditions must be met.

▶ **To enter intelligent mouse mode:**

- Choose Mouse > Intelligent.

Intelligent Mouse Synchronization Conditions

The Intelligent Mouse Synchronization command, available on the Mouse menu, automatically synchronizes mouse cursors during moments of inactivity. For this to work properly, however, the following conditions must be met:

- The active desktop should be disabled on the target.
- No windows should appear in the top left corner of the target page.
- There should not be an animated background in the top left corner of the target page.
- The target mouse cursor shape should be normal and not animated.
- The target mouse speeds should not be set to very slow or very high values.
- Advanced mouse properties such as "Enhanced pointer precision" or "Snap mouse to default button in dialogs" should be disabled.
- Choose "Best Possible Video Mode" in the Video Settings window.
- The edges of the target video should be clearly visible (that is, a black border should be visible between the target desktop and the remote KVM console window when you scroll to an edge of the target video image).
- When using the intelligent mouse synchronization function, having a file icon or folder icon located in the upper left corner of your desktop may cause the function not to work properly. To be sure to avoid any problems with this function, Raritan recommends you do not have file icons or folder icons in the upper left corner of your desktop.

After autosensing the target video, manually initiate mouse synchronization by clicking the Synchronize Mouse button on the toolbar. This also applies when the resolution of the target changes if the mouse cursors start to desync from each other.

If intelligent mouse synchronization fails, this mode will revert to standard mouse synchronization behavior.

Please note that mouse configurations will vary on different target operating systems. Consult your OS guidelines for further details. Also note that intelligent mouse synchronization does not work with UNIX targets.

Absolute Mouse Mode

In this mode, absolute coordinates are used to keep the client and target cursors in sync, even when the target mouse is set to a different acceleration or speed. This mode is supported on servers with USB ports and is the default mode for VM and dual VM targets.

▶ **To enter absolute mouse mode:**

- Choose Mouse > Absolute.

Note: The absolute mouse setting requires a USB target system and is the recommended mouse setting for KX II-101.

Note: Absolute Mouse Synchronization is available for use with the virtual media-enabled USB CIM (D2CIM-VUSB and D2CIM-DVUSB) only.

Single Mouse Cursor

Single Mouse mode uses only the target server mouse cursor and the local mouse pointer no longer appears onscreen. While in single mouse mode, the Synchronize Mouse command is not available (there is no need to synchronize a single mouse cursor).

Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See VKC Toolbar for the KX II-101 for additional information.

▶ **To enter single mouse mode, do the following:**

1. Choose Mouse > Single Mouse Cursor.

2. Click the Single/Double Mouse Cursor button ⌐ in the toolbar.

▶ **To exit single mouse mode:**

1. Press Ctrl+Alt+O on your keyboard to exit single mouse mode.

VKC Virtual Media

See the chapter on **Virtual Media** (on page 90) for complete information about setting up and using virtual media.

Smart Cards

For a list of supported smart cards, smart card readers, and additional system requirements, see **Supported and Unsupported Smart Card Readers** (on page 282).

When accessing a server remotely, you will have the opportunity to select an attached smart card reader and mount it onto the server. Smart card authentication is used with the target server, it is not used to log into the device. Therefore, changes to smart card PIN and credentials do not require updates to device accounts. When mounted onto the target server, the card reader and smart card will cause the server to behave as if they had been directly attached. Removal of the smart card or smart card reader will cause the user session to be locked or you will be logged out depending on how the card removal policy has been setup on the target server OS. When the KVM session is terminated, either because it has been closed or because you switch to a new target, the smart card reader will be automatically unmounted from the target server.

When PC-Share mode is enabled on the device, multiple users can share access to a target server. However, when a smart card reader is connected to a target, the device will enforce privacy regardless of the PC-Share mode setting. In addition, if you join a shared session on a target server, the smart card reader mounting will be disabled until exclusive access to the target server becomes available.

After a KVM session is established to the target server, a Smart Card menu and button are available in the Virtual KVM Client (VKC), Active KVM Client (AKC) and Multi-Platform Client (MPC). Once the menu is opened or the Smart Card button is selected, the smart card readers that have been detected as attached to the remote client are displayed. From this dialog you can attach additional smart card readers, refresh the list of smart card readers attached to the target, and detach smart card readers. You are also able to remove or reinsert a smart card. This function can be used to provide notification to a target server OS that requires a removal/reinsertion in order to display the appropriate login dialog. Using this function allows the notification to be sent to a single target without affecting other active KVM sessions.

▶ **To mount a smart card reader:**

1. Click the Smart Card menu and then select Smart Card Reader.

   Alternatively, click the Smart Card button [icon] in the toolbar.

2. Select the smart card reader from the Select Smart Card Reader dialog.

3. Click Mount.

4. A progress dialog will open. Check the 'Mount selected card reader automatically on connection to targets' checkbox to mount the smart card reader automatically the next time you connect to a target. Click OK to begin the mounting process.

> ► **To update the smart card in the Select Smart Card Reader dialog:**

* Click Refresh List if a new smart card reader has been attached to the client PC.

> ► **To send smart card remove and reinsert notifications to the target:**

* Select the smart card reader that is currently mounted and click the Remove/Reinsert button.

> ► **To unmount a smart card reader:**

* Select the smart card reader to be unmounted and click the Unmount button.

Smart card reader mounting is also supported from the Local Console. See **Local Console Smart Card Access** (on page 242).
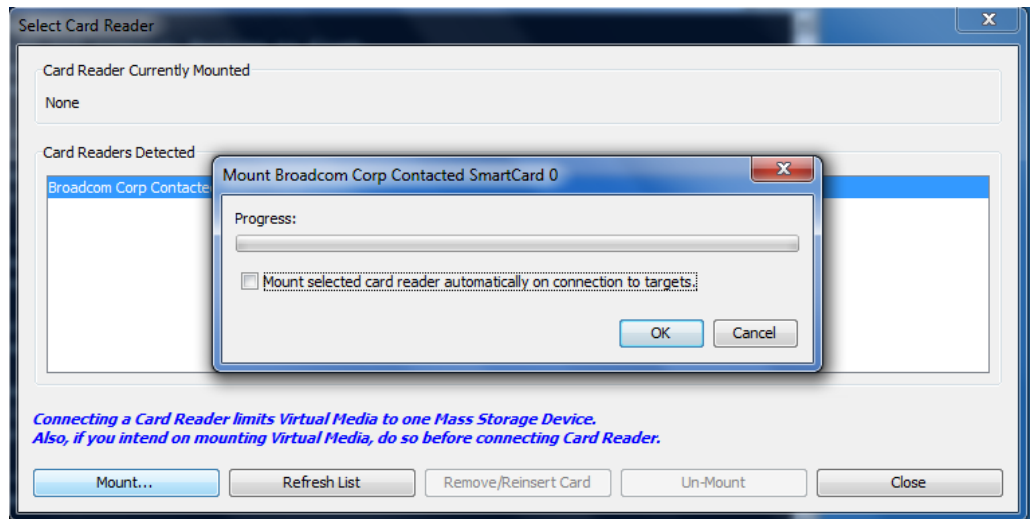
Tool Options

From the Tools menu, you can specify certain options for use with the Virtual KVM Client, including logging, setting the keyboard type, and defining hot keys for exiting Full Screen mode and Single Cursor mode.

> ► **To set the tools options:**

1. Choose Tools > Options. The Options dialog appears.

2. Select the Enable Logging checkbox only if directed to by Technical Support. This option creates a log file in your home directory.

3. Choose the Keyboard Type from the drop-down list (if necessary). The options include:

- US/International
- French (France)
- German (Germany)
- Japanese
- United Kingdom
- Korean (Korea)
- French (Belgium)
- Norwegian (Norway)
- Portuguese (Portugal)
- Danish (Denmark)
- Swedish (Sweden)
- German (Switzerland)
- Hungarian (Hungary)
- Spanish (Spain)
- Italian (Italy)
- Slovenian
- Translation: French - US
- Translation: French - US International

Note: In AKC, the keyboard type defaults to the local client, so this option does not apply.

4. Exit Full Screen Mode - Hotkey. When you enter Full Screen mode, the display of the target server becomes full screen and acquires the same resolution as the target server. This is the hot key used for exiting this mode.

5. Exit Single Cursor Mode - Hotkey. When you enter single cursor mode, only the target server mouse cursor is visible. This is the hot key used to exit single cursor mode and bring back the client mouse cursor. Click OK.

6. **Client Launch Settings**

7. Select the Client Launch Settings tab.

   a. To configure the target window settings:

   - Select 'Standard - sized to target Resolution' to open the window using the target's current resolution. If the target resolution is greater than the client resolution, the target window covers as much screen area as possible and scroll bars are added (if needed).

   - Select Full Screen to open the window in full screen mode.

a. To configure the monitor on which the target viewer is launched:

  ▪ Select 'Monitor Client Was Launched from' if you want the target viewer to be launched using the same display as the application that is being used on the client (for example, a web browser or applet).

8. Use Select From Detected Monitors to select from a list of target monitors that are currently detected by the application. If a previously selected monitor is no longer detected, 'Currently Selected Monitor Not Detected' is displayed.

9. Click OK.

Keyboard Limitations

Slovenian Keyboards

The < key does not work on Slovenian keyboards due to a JRE limitation.

Language Configuration on Linux

Because the Sun JRE on Linux has problems generating the correct Key Events for foreign-language keyboards configured using System Preferences, Raritan recommends that you configure foreign keyboards using the methods described in the following table.

Language	Configuration method
US Intl	Default
French	Keyboard Indicator
German	System Settings (Control Center)
Japanese	System Settings (Control Center)
UK	System Settings (Control Center)
Korean	System Settings (Control Center)
Belgian	Keyboard Indicator
Norwegian	Keyboard Indicator
Danish	Keyboard Indicator
Swedish	Keyboard Indicator
Hungarian	System Settings (Control Center)
Spanish	System Settings (Control Center)
Italian	System Settings (Control Center)
Slovenian	System Settings (Control Center)
Portuguese	System Settings (Control Center)

Note: The Keyboard Indicator should be used on Linux systems using Gnome as a desktop environment.

View Options

View Toolbar

You can use the Virtual KVM client with or without the toolbar display.

▶ **To toggle the display of the toolbar (on and off):**

- Choose View > View Toolbar.

Scaling

Scaling your target window allows you to view the entire contents of the target server window. This feature increases or reduces the size of the target video to fit the Virtual KVM Client window size, and maintains the aspect ratio so that you see the entire target server desktop without using the scroll bar.

▶ **To toggle scaling (on and off):**

- Choose View > Scaling.

Target Screen Resolution

When you enter Full Screen mode, the target's full screen is displayed and acquires the same resolution as the target server. The hot key used for exiting this mode is specified in the Options dialog (the default is Ctrl+Alt+M). While in Full Screen mode, moving your mouse to the top of the screen will display the Full Screen mode menu bar.

▶ **To enter full screen mode:**

- Choose View > Full Screen.

▶ **To exit full screen mode:**

- Press the hot key configured in the Tools Options dialog. The default is Ctrl+Alt+M. For AKC, select Connection/Exit from the hidden menu bar, which is accessed by hovering your mouse at the top of the screen.

Alternatively, if you want to access the target in full screen mode at all times, you can make Full Screen mode the default.

▶ **To set Full Screen mode as the default mode:**

1. Click Tools > Options to open the Options dialog.

2. Select Enable Launch in Full Screen Mode and click OK.

Help Options

About Raritan Virtual KVM Client

This menu command provides version information about the Virtual KVM Client, in case you require assistance from Raritan Technical Support.

▶   **To obtain version information:**

1. Choose Help > About Raritan Virtual KVM Client.

2. Use the Copy to Clipboard button to copy the information contained in the dialog to a clipboard file so it can be accessed later when dealing with support (if needed).

Active KVM Client (AKC)

Please note this client is used by various Raritan products. As such, references to other products may appear in this section of help since they are shared between products.

Overview

AKC is based on Microsoft Windows .NET technology and allows users to run the client in Windows environments without the use of the Java Runtime Environment (JRE), which is required to run Raritan's Virtual KVM and Multi-Platform clients. AKC also works with CC-SG.

AKC and VKC share similar features with the exception of the following:

*   Minimum system requirements

*   Supported operating systems and browsers

*   Keyboard macros created in AKC cannot be used in VKC.

See the *Virtual KVM Client* (see "*Virtual KVM Client (VKC)*" on page 53) section for information on using the available features of the application. If there is a difference between how AKC functions as compared to VKC, it is noted in the topic.

Also see *Enabling Direct Port Access*   (see "*Enabling Direct Port Access via URL*" on page 142)and *Enabling the AKC Download Server Certificate Validation* (on page 146) for configuration information on using AKC.

Note: If you are using direct port access with AKC, you must open a new browser window or browser tab for each target you want to access. If you try to access another target by entering the DPA URL into the same browser window or browser tab you are currently accessing a target from, you will not be able to connect and may receive an error.

AKC Supported .NET Framework, Operating Systems and Browsers

.NET Framework

AKC requires Windows .NET® version 3.5, and will work with both 3.5 and 4.0 installed.

Operating Systems

AKC is compatible with the following platforms running .NET Framework 3.5:

- Windows XP® operating system
- Windows Vista® operating system (up to 64 bit)
- Windows 7® operating system   (up to 64 bit)

Note: You must be using Windows 7 if WINDOWS PC FIPs is turned on and you are accessing a target using AKC and a smartcard.

Since .NET is required to run AKC, if you do not have .NET installed or you have an unsupported version of .NET installed, you will receive a message instructing you to check the .NET version.

Browser
- Internet Explorer 6 or later

If you attempt to open AKC from a browser other than IE 6 or later, you will receive an error message instructing you to check your browser and to switch to Internet Explorer.

Prerequisites for Using AKC

In order to use AKC:

- Ensure the cookies from the IP address of the device that is being accessed are not currently being blocked.

- Windows Vista, Windows 7 and Windows 2008 server users should ensure that the IP address of the device being accessed is included in their browser's Trusted Sites Zone and that Protected Mode is not on when accessing the device.

Enable AKC Download Server Certificate Validation

If the device (or CC-SG) administrator has enabled the Enable AKC Download Server Certificate Validation option:

- Administrators must upload a valid certificate to the device or generate a self-signed certificate on the device. The certificate must have a valid host designation.

- Each user must add the CA certificate (or a copy of self-signed certificate) to the Trusted Root CA store in their browser.

When launching AKC from the CC-SG Admin Client, you must have JRE™ 1.6.0_10 or above.

Multi-Platform Client (MPC)

Raritan Multi-Platform Client (MPC) is a graphical user interface for the Raritan product lines, providing remote access to target servers connected to Raritan KVM over IP devices. For details on using MPC, see the **KVM and Serial Access Clients Guide** available on Raritan's website on the same page as the user guide. Instructions on launching MPC are provided there.

Please note this client is used by various Raritan products. As such, references to other products may appear in this section of help since they are shared between products.

Launching MPC from a Web Browser

Important: Regardless of the browser you use, you must allow pop-ups from the Dominion device's IP address in order to open MPC.

Important: Only Mac 10.5 and 10.6 with an Intel® processor can run JRE 1.6 and, therefore, be used as a client. Mac 10.5.8 does not support MPC as a standalone client.

1. To open MPC from a client running any supported browser, type http://IP-ADDRESS/mpc into the address line, where IP-ADDRESS is the IP address of your Raritan device. MPC will open in a new window.

   Note: The Alt+Tab command will toggle between windows only on the local system.

   When MPC opens, the Raritan devices that were automatically detected and which are found on your subnet are displayed in the Navigator in tree format.

2. If your device is not listed by name in the navigator, add it manually:

   a. Choose Connection > New Profile. The Add Connection window opens.

   b. In the Add Connection window, type a device Description, specify a Connection Type, add the device IP address, and click OK. These specifications can be edited later.

3. In the Navigator panel on the left of the page, double-click the icon that corresponds to your Raritan device to connect to it.

Note: Depending on your browser and browser security settings, you may see various security and certificate check and warning messages. It is necessary to accept the options in order to open MPC.

Note: If you are using Firefox 3.0.3, you may experience problems launching the application. If this occurs, clear the browser cache and launch the application again.

Raritan Serial Console (RSC)

The standalone Raritan Serial Console (RSC) is used to make direct connections to a serial target without going through the device. The user specifies the device address and the port number (target), and is then connected.

Opening RSC from the Remote Console

▶ **To open the Raritan Serial Console (RSC) from the Remote Console:**

1. Select the Port Access tab.

2. Click the name of the serial port you want to access for the RSC.

    Note: A security pop-up screen appears only if you used https to connect to the RSC.

3. If you're using Dominion DSX:

    ▪ Click Yes. A Warning - Security pop-up screen appears.

    ▪ Click Yes to access the Raritan Serial Console from the Port page.

    Note: If you click Always, you will not receive the security page for future access.

    ▪ The Raritan Serial Console window appears.

    If you're using Dominion KSX or KX:

    ▪ Click Connect to start connecting to the target port for RSC, and the Raritan Serial Console window appears.

    ▪ The Raritan Serial Console window appears.

Note: You can download the standalone Raritan Serial Console from the Raritan website (www.raritan.com) on the Support page.

▶ **To open RSC from the Windows® desktop:**

1. Double-click the shortcut or use the Start menu to open the standalone RSC. The Raritan Serial Console Login connection properties window appears.

2. Enter the device's IP address, account information, and the desired target (port).

3. Click Start. RSC opens with a connection to the port.

Note: If you experience unrecognized characters or blurry pages in the RSC window due to localization support, try changing the font to Courier New. Click Emulator > Settings > Display and select Courier New for Terminal Font Properties or GUI Font Properties.

Note: When RSC connects to a serial target, hitting Ctrl + _ or Ctrl + ^ + _ does not cause information to be sent. However, hitting the Ctrl + Shift + _ or the Ctrl + Shift + ^ will cause information to be sent.

▶ **To open RSC on Sun™ Solaris™:**

1. Open a terminal window and change to the directory where you installed the RSC.

2. Type `./start.sh` and press Enter to open RSC.

3. Double-click the desired device to establish a connection.

4. Type your user name and password.

5. Click OK to log on.

Chapter 4 Rack PDU (Power Strip) Outlet Control

In This Chapter

Overview

The KSX II allows you to control Raritan PX and RPC series rack PDU (power strip) outlets. Once a PX or RPC series is setup and then attached to the KSX II, the rack PDU and its outlets can be controlled from the Powerstrip page in the KSX II interface. This page is accessed by clicking on the Power menu at the top of the page.

The Powerstrip page will display rack PDUs attached to the KSX II for which the user has been granted appropriate port access permissions.

*Note: For information on setting up a PX, see the **Dominion PX User Guide**.*

From the Powerstrip page, you are able to turn the outlets on and off, as well as cycle their power. You are also able to view the following power strip and outlet information:

- Powerstrip Device Information:
    - Name
    - Model
    - Temperature
    - Current Amps
    - Maximum Amps
    - Voltage
    - Power in Watts
    - Power in Volts Ampere
- Outlet Display Information:
    - Name - Named assigned to the outlet when it was configured.
    - State - On or Off status of the outlet.
    - Control - Turn outlets on or off, or cycle their power.
    - Association - The ports associated with the outlet.

Initially, when you open the Powerstrip page, the power strips that are currently connected to the KSX II are displayed in the Powerstrip drop-down. Additionally, information relating to the currently selected power strip is displayed. If no power strips are connected to the KSX II, a message stating "No powerstrips found" will be displayed in the Powerstrip Device section of the page.

Turning Outlets On/Off and Cycling Power

▶   **To turn an outlet on:**

1. Click the Power menu to access the Powerstrip page.

2. From the Powerstrip drop-down, select the PX rack PDU (power strip) you want to turn on.

3. Click Refresh to view the power controls.

4. Click On.

Chapter 4: Rack PDU (Power Strip) Outlet Control

5. Click OK to close the Power On confirmation dialog. The outlet will be turned on and its state will be displayed as 'on'.
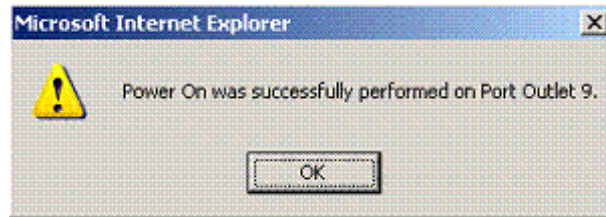
▶ **To turn an outlet off:**

1. Click Off.
2. Click OK on the Power Off dialog.
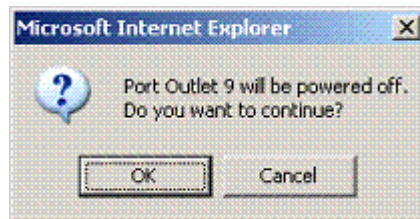
3. Click OK on the Power Off confirmation dialog. The outlet will be turned off and its state will be displayed as 'off'.

▶ **To cycle the power of an outlet:**

1. Click the Cycle button. The Power Cycle Port dialog opens.
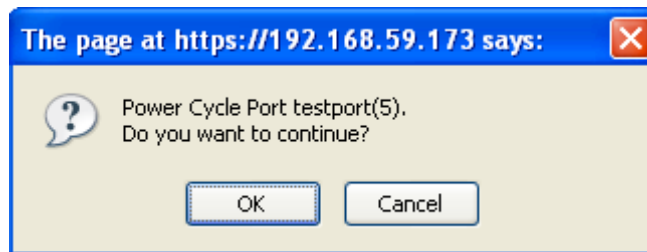
2. Click OK. The outlet will then cycle (note that this may take a few seconds).

The page at https://192.168.59.173 says:

⚠ Power Cycle was successfully performed on Port testport(5).

OK
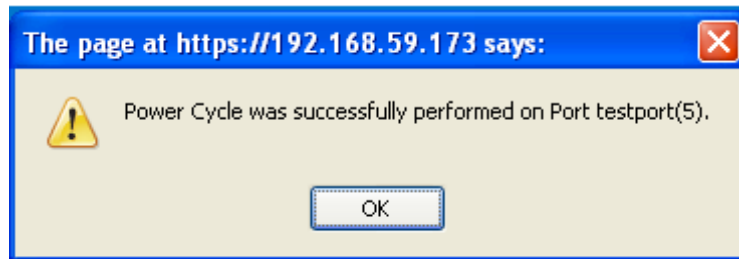
3. Once the cycling is complete the dialog will open. Click OK to close the dialog.

Chapter 5   Virtual Media

In This Chapter

Overview

Virtual media extends KVM capabilities by enabling KVM target servers to remotely access media from a client PC and network file servers. With this feature, media mounted on a client PC and network file servers is essentially "mounted virtually" by the target server. The target server can then read from and write to that media as if it were physically connected to the target server itself. In addition to data file support via virtual media files are supported by virtual media via a USB connection.

Virtual media can include internal and USB-mounted CD and DVD drives, USB mass storage devices, PC hard drives, and ISO images (disk images).

Note: ISO9660 is the standard supported by Raritan. However, other ISO standards can be used.

Virtual media provides the ability to perform additional tasks remotely, such as:

- Transferring files
- Running diagnostics
- Installing or patching applications
- Complete installation of the operating system

This expanded KVM control eliminates most trips to the data center, saving time and money, thereby making virtual media very powerful.
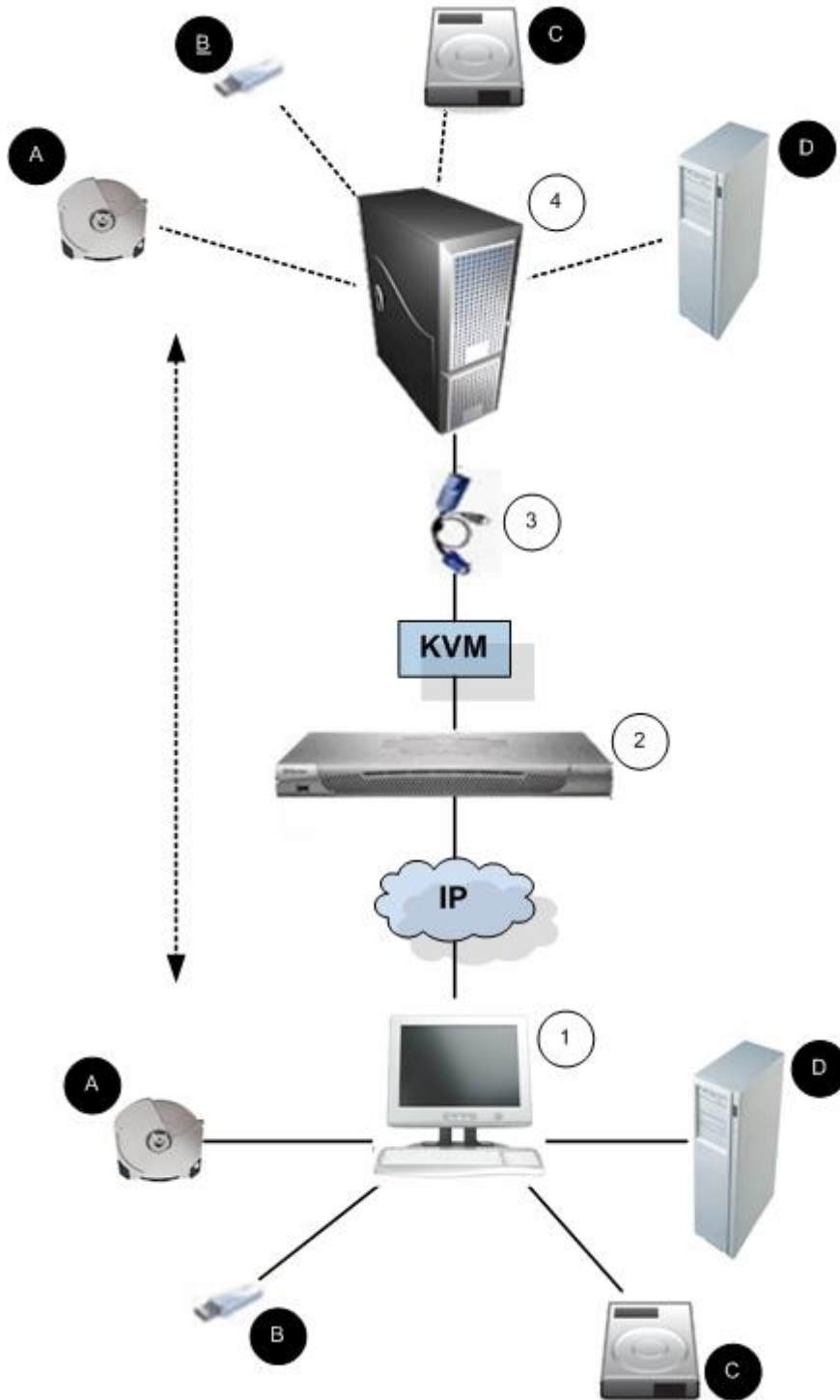
Diagram key

①	Desktop PC	Ⓐ	CD/DVD drive
②	KSX II	Ⓑ	USB mass storage device
③	CIM	Ⓒ	PC hard drive
④	Target server	Ⓓ	Remote file server (ISO images)

Prerequisites for Using Virtual Media

With the virtual media feature, you can mount up to two drives (of different types) that are supported by the USB profile currently applied to the target. These drives are accessible for the duration of the KVM session.

For example, you can mount a specific CD-ROM, use it, and then disconnect it when you are done. The CD-ROM virtual media "channel" will remain open, however, so that you can virtually mount another CD-ROM. These virtual media "channels" remain open until the KVM session is closed as long as the USB profile supports it.

To use virtual media, connect/attach the media to the client or network file server that you want to access from the target server. This need not be the first step, but it must be done prior to attempting to access this media.

The following conditions must be met in order to use virtual media:

Dominion Device

- For users requiring access to virtual media, the device permissions must be set to allow access to the relevant ports, as well as virtual media access (VM Access port permission) for those ports. Port permissions are set at the group-level.

- A USB connection must exist between the device and the target server.

- If you want to use PC-Share, **Security Settings** (on page 189) must also be enabled in the Security Settings page. **Optional**

- You must choose the correct USB profile for the KVM target server you are connecting to.

Client PC

- Certain virtual media options require administrative privileges on the client PC (for example, drive redirection of complete drives).

Note: If you are using Microsoft Vista or Windows 7, disable User Account Control or select Run as Administrator when starting Internet Explorer. To do this, click the Start Menu, locate IE, right-click and select Run as Administrator.

Target Server

- KVM target servers must support USB connected drives.

- KVM target servers running Windows 2000 must have all of the recent patches installed.

- USB 2.0 ports are both faster and preferred.

Using Virtual Media via VKC and AKC in a Windows Environment

Windows XP® operating system administrator and standard user privileges vary from those of the Windows Vista® operating system and the Windows 7® operating system.

When enabled in Vista or Windows 7, User Access Control (UAC) will provide the lowest level of rights and privileges a user needs for an application. For example, a Run as Administrator option is provided for Internet Explorer® form Administrator level tasks, otherwise these will not be accessible even though the user has an Administrator login.

Both of these features affect the types of virtual media that can be accessed by users via Virtual KVM Client (VKC) and Active KVM Client (AKC). See your Microsoft® help for additional information on these features and how to use them.

Following is a list virtual media types users can access via VKC and AKC when running in a Windows environment. The features are broken down by client and the virtual media features that are accessible to each Windows user role.

Windows XP

If you are running VKC and AKC in a Windows XP environment, users must have Administrator privileges to access any virtual media type other than CD-ROM connections, ISOs and ISO images.

Windows Vista and Windows 7

If you are running VKC and AKC in a Windows Vista or Windows 7 environment and UAC is enabled, the following virtual media types can be accessed depending on the user's Windows role:

Client	Administrator	Standard User
AKC and VKC	Access to: • Fixed drives and fixed drive partitions • Removable drives • CD/DVD drives • ISO images • Remote ISO images	Access to: • Removable drives • CD/DVD drives • ISO images • Remote ISO images

Using Virtual Media

With the KSX II virtual media feature, you can mount up to two drives (of different types). These drives are accessible for the duration of the KVM session.

For example, you can mount a specific CD-ROM, use it, and then disconnect it when you are done. The CD-ROM virtual media "channel" will remain open, however, so that you can virtually mount another CD-ROM. These virtual media "channels" remain open until the KVM session is closed.

▶ **To use virtual media:**

1. Connect/attach the media to the client or network file server that you want to access from the target server. This need not be the first step, but it must be done prior to attempting to access this media.

2. Verify that the appropriate prerequisites are met. See ***Prerequisites for Using Virtual Media*** (on page 94).

3. The following conditions must be met in order to use virtual media:

KSX II

- For users requiring access to virtual media, KSX II permissions must be set to allow access to the relevant ports, as well as virtual media access (VM Access port permission) for those ports. Port permissions are set at the group-level; refer to Setting Port Permissions in the device user guide for more information.

- A USB connection must exist between the KSX II device and the target server.

- If you want to use PC-Share, ***Security Settings*** (on page 189) must also be enabled in the Security Settings page. **Optional**

- You must choose the correct USB profile for the KVM target server you are connecting to.

Client PC

- Certain virtual media options require administrative privileges on the client PC (for example, drive redirection of complete drives).

    Note: If you are using Microsoft® Vista, turn User Account Control off: Control Panel > User Accounts > User Account Control > turn off.

    If you would prefer not to change Vista account permissions, run Internet Explorer® as an administrator. To do this, click the Start Menu, locate IE, right-click it and select Run as Administrator.

Target Server

- KVM target servers must support USB connected drives.

- KVM target servers running the Windows 2000® operating system must have all of the recent patches installed.

1. USB 2.0 ports are both faster and preferred..

2. If you plan to access file server ISO images, identify those file servers and images through the KSX II Remote Console File Server Setup page. See *File Server Setup (File Server ISO Images Only)* (on page 98).

Note: ISO9660 format is the standard supported by Raritan. However, other CD-ROM extensions may also work.

3. Open a KVM session with the appropriate target server.

   a. Open the Port Access page from the KSX II Remote Console.

   b. Connect to the target server from the Port Access page:

   - Click the Port Name for the appropriate server.

   - Choose the Connect command from the Port Action menu. The target server opens in a *Virtual KVM Client* (see "*Virtual KVM Client (VKC)*" on page 53) window.

4. Connect to the virtual media.

For:	Select this VM option:
Local drives	Connect Drive
Local CD/DVD drives	*Connect CD-ROM/ISO Image* (see "*CD-ROM/DVD-ROM/ISO Images*" on page 101)
ISO Images	Connect CD-ROM/ISO Image
File Server ISO Images	Connect CD-ROM/ISO Image

5. Upon completion of your tasks, disconnect the virtual media. See *Disconnecting Virtual Media* (on page 103).

File Server Setup (File Server ISO Images Only)

Note: This feature is only required when using virtual media to access file server ISO images. ISO9660 format is the standard supported by Raritan. However, other CD-ROM extensions may also work.

Note: SMB/CIFS support is required on the file server.

Use the Remote Console File Server Setup page to designate the files server(s) and image paths that you want to access using virtual media. File server ISO images specified here are available for selection in the Remote Server ISO Image Hostname and Image drop-down lists in the Map Virtual Media CD/ISO Image dialog. See **CD-ROM/DVD-ROM/ISO Images**.

▶ **To designate file server ISO images for virtual media access:**

1. Choose Virtual Media from the Remote Console. The File Server Setup page opens.

2. Check the Selected checkbox for all media that you want accessible as virtual media.

3. Enter information about the file server ISO images that you want to access:

   - IP Address/Host Name - Host name or IP address of the file server.

   - Image Path - Full path name of the location of the ISO image. For example, /sharename0/path0/image0.iso, \sharename1\path1\image1.iso, and so on.

   Note: The host name cannot exceed 232 characters in length.

4. Click Save. All media specified here will now be available for selection in the Map Virtual Media CD/ISO Image dialog.

Note: You cannot access a remote ISO image via virtual media using an IPv6 address due to technical limitations of third-party software used by the by the KX, KSX or KX101 G2 device.

Note: If you are connecting to a Windows 2003® server and attempt to load an ISO image from the server, you may receive an error stating "Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password". If this occurs, disable "Microsoft Network Server: Digitally Sign Communications".

File Server Setup

IP Address/Host Name: Enter name of the host name or IP Address of shared drive containing ".iso" image.
Image Path: Enter path to ".iso" image on shared drive. Do not include host name or IP Address in the path.

Selected	Host Name/IPAddress	Image Path
☐		
☐		
☐		
☐		
☐		
☐		
☐		
☐		
☐		
☐		

Save   Cancel

Connecting to Virtual Media

Local Drives

This option mounts an entire drive, which means the entire disk drive is mounted virtually onto the target server. Use this option for hard drives and external drives only. It does not include network drives, CD-ROM, or DVD-ROM drives. This is the only option for which Read/Write is available.

Note: KVM target servers running certain versions of the Windows operating system may not accept new mass storage connections after an NTFS-formatted partition (for example, the local C drive) has been redirected to them.

If this occurs, close the Remote Console and reconnect before redirecting another virtual media device. If other users are connected to the same target server, they must also close their connections to the target server.

Note: In the KSX II 2.3.0 and above, when you mount an external drive such as a floppy drive, the LED light on the drive will remain on because the device is checking the drive every 500 milliseconds to verify the drive is still mounted.

▶ **To access a drive on the client computer:**

1. From the Virtual KVM Client, choose Virtual Media > Connect Drive. The Map Virtual Media Drive dialog appears.
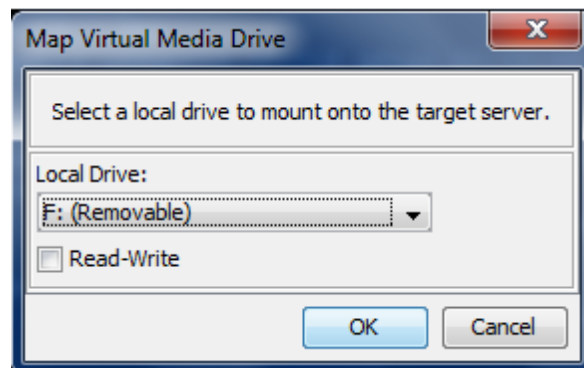
2. Choose the drive from the Local Drive drop-down list.

3. If you want Read and Write capabilities, select the Read-Write checkbox. This option is disabled for nonremovable drives. See the **Conditions when Read/Write is Not Available** (on page 101) for more information. When checked, you will be able to read or write to the connected USB disk.

> *WARNING: Enabling Read/Write access can be dangerous!*
> *Simultaneous access to the same drive from more than one entity*
> *can result in data corruption. If you do not require Write access,*
> *leave this option unselected.*

4. Click Connect. The media will be mounted on the target server virtually. You can access the media just like any other drive.

Conditions when Read/Write is Not Available

Virtual media Read/Write is not available in the following situations:

- For all hard drives.

- When the drive is write-protected.

- When the user does not have Read/Write permission:

    - Port Permission Access is set to None or View.

    - Port Permission VM Access is set to Read-Only or Deny.

CD-ROM/DVD-ROM/ISO Images

This option mounts CD-ROM, DVD-ROM, and ISO images.

Note: ISO9660 format is the standard supported by Raritan. However, other CD-ROM extensions may also work.

▶ To access a CD-ROM, DVD-ROM, or ISO image:

1. From the Virtual KVM Client, choose Virtual Media > Connect CD-ROM/ISO Image. The Map Virtual Media CD/ISO Image dialog appears.

2. For internal and external CD-ROM or DVD-ROM drives:

   a. Choose the Local CD/DVD Drive option.

   b. Choose the drive from the Local CD/DVD Drive drop-down list. All available internal and external CD and DVD drive names will be populated in the drop-down list.

   c. Click Connect.

3. For ISO images:

   a. Choose the ISO Image option. Use this option when you want to access a disk image of a CD, DVD, or hard drive. ISO format is the only format supported.

   b. Click the Browse button.

   c. Navigate to the path containing the disk image you want to use and click Open. The path is populated in the Image Path field.

   d. Click Connect.

4. For remote ISO images on a file server:

   a. Choose the Remote Server ISO Image option.

   b. Choose Hostname and Image from the drop-down list. The file servers and image paths available are those that you configured using the File Server Setup page. Only items you configured using the File Server Setup page will be in the drop-down list.

   c. File Server Username - User name required for access to the file server. The name can include the domain name such as mydomain/username.

   d. File Server Password - Password required for access to the file server (field is masked as you type).

   e. Click Connect.

   The media will be mounted on the target server virtually. You can access the media just like any other drive.

Note: If you are working with files on a Linux® target, use the Linux Sync command after the files are copied using virtual media in order to view the copied files. Files may not appear until a sync is performed.

Note: If you are using the Windows 7® operating system®, Removable Disk is not displayed by default in the Window's My Computer folder when you mount a Local CD/DVD Drive or Local or Remote ISO Image. To view the Local CD/DVD Drive or Local or Remote ISO Image in this folder, select Tools > Folder Options > View and deselect "Hide empty drives in the Computer folder".

Note: You cannot access a remote ISO image via virtual media using an IPv6 address due to technical limitations of third-party software used by the KSX II.

Disconnecting Virtual Media

> ► **To disconnect the virtual media drives:**

- For local drives, choose Virtual Media > Disconnect Drive.

- For CD-ROM, DVD-ROM, and ISO images, choose Virtual Media > Disconnect CD-ROM/ISO Image.

Note: In addition to disconnecting the virtual media using the Disconnect command, simply closing the KVM connection closes the virtual media as well.

Chapter 6   USB Profiles

In This Chapter

Overview

To broaden the KSX II's compatibility with different KVM target servers, Raritan provides a standard selection of USB configuration profiles for a wide range of operating system and BIOS-level server implementations.

The Generic (default) USB profile meets the needs of the vast majority of deployed KVM target server configurations. Additional profiles are provided to meet the specific needs of other commonly deployed server configurations (for example, Linux® and Mac OS X®). There are also a number of profiles (designated by platform name and BIOS revision) to enhance virtual media function compatibility with the target server, for example, when operating at the BIOS level.

USB profiles are configured on the Device Settings > Port Configuration > Port page of the KSX II Remote and Local Consoles. A device administrator can configure the port with the profiles that best meet the needs of the user and the target server configuration.

A user connecting to a KVM target server chooses among these preselected profiles in the *Virtual KVM Client* (see "*Virtual KVM Client (VKC)*" on page 53), depending on the operational state of the KVM target server. For example, if the server is running and the user wants to use the Windows® operating system, it would be best to use the Generic profile. But if the user wants to change settings in the BIOS menu or boot from a virtual media drive, depending on the target server model, a BIOS profile may be more appropriate.

Should none of the standard USB profiles provided by Raritan work with a given KVM target, please contact Raritan Technical Support for assistance.

CIM Compatibility

In order to make use of USB profiles, you must use a D2CIM-VUSB or D2CIM-DVUSB with updated firmware. A VM-CIM that has not had its firmware upgraded will support a broad range of configurations (Keyboard, Mouse, CD-ROM, and Removable Drive) but will not be able to make use of profiles optimized for particular target configurations. Given this, existing VM-CIMs should be upgraded with latest firmware in order to access USB profiles. Until existing VM-CIMs are upgraded, they will be able to provide functionality equivalent to the 'Generic' profile.

VM-CIM firmware is automatically upgraded during a KSX II firmware upgrade, but VM-CIMs that have not had their firmware upgraded can be upgraded as described in **Upgrading CIMs** (on page 211).

See **Computer Interface Modules (CIM) Specifications** (see "**Computer Interface Modules (CIMs)**" on page 274) for additional information.

Available USB Profiles

The current release of the KSX II comes with the selection of USB profiles described in the following table. New profiles are included with each firmware upgrade provided by Raritan. As new profiles are added, they will be documented in the help.

USB profile	Description
BIOS Dell® PowerEdge® 1950/2950/2970/6950/R200	Dell PowerEdge 1950/2950/2970/6950/R200 BIOS Use either this profile or 'Generic' profile for Dell PowerEdge 1950/2950/2970/6950/R200 BIOS. Restrictions: • None
BIOS Dell OptiPlex ™ Keyboard Only	Dell OptiPlex BIOS Access (Keyboard Only) Use this profile to have keyboard functionality for the Dell OptiPlex BIOS when using D2CIM-VUSB. When using the new D2CIM-DVUSB, use 'Generic' profile. Notice: • Optiplex 210L/280/745/GX620 requires D2CIM-DVUSB with 'Generic' profile to support virtual media

USB profile	Description
	Restrictions:
	• USB bus speed limited to full-speed (12 MBit/s)
	• No virtual media support
BIOS DellPowerEdge Keyboard Only	Dell PowerEdge BIOS Access (Keyboard Only)
	Use this profile to have keyboard functionality for the Dell PowerEdge BIOS when using D2CIM-VUSB. When using the new D2CIM-DVUSB, use 'Generic' profile.
	Notice:
	• PowerEdge 650/1650/1750/2600/2650 BIOS do not support USB CD-ROM and disk drives as a bootable device
	• PowerEdge 750/850/860/1850/2850/SC1425 BIOS requires D2CIM-DVUSB with 'Generic' profile to support virtual media
	• Use 'BIOS Dell PowerEdge 1950/2950/2970/6950/R200' or 'Generic' profile for PowerEdge 1950/2950/2970/6950/R200 when operating in the BIOS
	Restrictions:
	• USB bus speed limited to full-speed (12 MBit/s)
	• Absolute mouse synchronization™ not supported
	• No virtual media support
BIOS ASUS P4C800 Motherboard	Use this profile to access BIOS and boot from Virtual Media on Asus P4C800-based systems.
	Restrictions:
	• USB bus speed limited to full-speed (12 MBit/s)
	• Virtual CD-ROM and disk drives cannot be used simultaneously

USB profile	Description
BIOS Generic	BIOS Generic Use this profile when Generic OS profile does not work on the BIOS. WARNING: USB enumeration will trigger whenever virtual media is connected or disconnected. Restrictions: • USB bus speed limited to full-speed (12 MBit/s) • Absolute mouse synchronization™ not supported • Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS HP® Proliant™ DL145	HP Proliant DL145 PhoenixBIOS Use this profile for HP Proliant DL145 PhoenixBIOS during OS installation. Restrictions: • USB bus speed limited to full-speed (12 MBit/s)
BIOS HP Compaq® DC7100/DC7600	BIOS HP Compaq DC7100/DC7600 Use this profile to boot the HP Compaq DC7100/DC7600 series desktops from virtual media. Restrictions: • Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS IBM ThinkCentre Lenovo	IBM Thinkcentre Lenovo BIOS Use this profile for the IBM® Thinkcentre Lenovo system board (model 828841U) during BIOS operations. Restrictions: • USB bus speed limited to full-speed (12 MBit/s) • Virtual CD-ROM and disk drives cannot be used simultaneously
IBM BladeCenter H with Advanced Management	Use this profile to enable virtual media functionality when D2CIM-VUSB or

USB profile	Description
Module	D2CIM-DVUSB is connected to the Advanced Management Module. Restrictions: • Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS Lenovo ThinkPad T61 & X61	BIOS Lenovo ThinkPad T61 and X61 (boot from virtual media) Use this profile to boot the T61 and X61 series laptops from virtual media. Restrictions: • USB bus speed limited to full-speed (12 MBit/s)
BIOS Mac	BIOS Mac Use this profile for Mac® BIOS. Restrictions: • Absolute mouse synchronization™ not supported • Virtual CD-ROM and disk drives cannot be used simultaneously
Generic	The generic USB profile resembles the behavior of the original KX2 release. Use this for Windows 2000® operating system, Windows XP® operating system, Windows Vista® operating system and later. Restrictions: • None
HP Proliant DL360/DL380 G4 (HP SmartStart CD)	HP Proliant DL360/DL380 G4 (HP SmartStart CD) Use this profile for the HP Proliant DL360/DL380 G4 series server when installing OS using HP SmartStart CD. Restrictions: • USB bus speed limited to full-speed (12 MBit/s) • Absolute mouse synchronization™ not supported
HP Proliant DL360/DL380 G4 (Windows 2003® Server	HP Proliant DL360/DL380 G4 (Windows 2003 Server Installation)

USB profile	Description
Installation)	Use this profile for the HP Proliant DL360/DL380 G4 series server when installing Windows 2003 Server without the help of HP SmartStart CD. Restrictions: • USB bus speed limited to full-speed (12 MBit/s)
Linux®	Generic Linux profile This is the generic Linux profile; use it for Redhat Enterprise Linux, SuSE Linux Enterprise Desktop and similar distributions. Restrictions: • Absolute mouse synchronization™ not supported
MAC OS X® (10.4.9 and later)	Mac OS-X, version 10.4.9 and later This profile compensates the scaling of mouse coordinates introduced in recent versions of Mac OS-X. Select this if the remote and local mouse positions get out of sync near the desktop borders. Restrictions: • Virtual CD-ROM and disk drives cannot be used simultaneously
RUBY Industrial Mainboard (AwardBIOS)	RUBY Industrial Mainboard (AwardBIOS) Use this profile for the RUBY-9715VG2A series industrial mainboards with Phoenix/AwardBIOS v6.00PG. Restrictions: • USB bus speed limited to full-speed (12 MBit/s) • Virtual CD-ROM and disk drives cannot be used simultaneously
Supermicro Mainboard Phoenix (AwardBIOS)	Supermicro Mainboard Phoenix AwardBIOS Use this profile for the Supermicro series mainboards with Phoenix AwardBIOS.

USB profile	Description
	Restrictions:
	• Virtual CD-ROM and disk drives cannot be used simultaneously
Suse 9.2	SuSE Linux 9.2
	Use this for SuSE Linux 9.2 distribution.
	Restrictions:
	• Absolute mouse synchronization™ not supported
	• USB bus speed limited to full-speed (12 MBit/s)
Troubleshooting 1	Troubleshooting Profile 1
	• Mass Storage first
	• Keyboard and Mouse (Type 1)
	• USB bus speed limited to full-speed (12 MBit/s)
	• Virtual CD-ROM and disk drives cannot be used simultaneously
	WARNING: USB enumeration will trigger whenever virtual media is connected or disconnected.
Troubleshooting 2	Troubleshooting Profile 2
	• Keyboard and Mouse (Type 2) first
	• Mass Storage
	• USB bus speed limited to full-speed (12 MBit/s)
	• Virtual CD-ROM and disk drives cannot be used simultaneously
	WARNING: USB enumeration will trigger whenever virtual media is connected or disconnected.
Troubleshooting 3	Troubleshooting Profile 3
	• Mass Storage first
	• Keyboard and Mouse (Type 2)
	• USB bus speed limited to full-speed (12 MBit/s)

USB profile	Description
	• Virtual CD-ROM and disk drives cannot be used simultaneously
	WARNING: USB enumeration will trigger whenever virtual media is connected or disconnected.
Use Full Speed for Virtual Media CIM	Use Full Speed for virtual media CIM This profile resembles the behavior of the original KX2 release with Full Speed for virtual media CIM option checked. Useful for BIOS that cannot handle High Speed USB devices. Restrictions: • USB bus speed limited to full-speed (12 MBit/s)

Selecting Profiles for a KVM Port

The KSX II comes with a set of USB profiles that you can assign to a KVM port based on the characteristics of the KVM target server it connects to. You assign USB profiles to a KVM port in the Device Settings > Port Configuration > Port page in either the KSX II Remote or Local Console.

It is the administrator that designates the profiles that are most likely to be needed for a specific target. These profiles are then available for selection via MPC, AKC and VKC. If a profile has not been made available, you can access any of the available profiles by selecting USB Profile > Other Profiles.

Assigning USB profiles to a KVM port makes those profiles available to a user when connected to a KVM target server. If required, the user can select a USB profile from the USB Profile menu in VKC, AKC or MPC.

For information about assigning USB profiles to a KVM port, see *Configuring USB Profiles (Port Page)* (on page 181).

Mouse Modes when Using the Mac OS-X USB Profile with a DCIM-VUSB

If you are using a DCIM-VUSB, using a Mac OS-X® USB profile, and running Mac OS-X 10.4.9 (or later), when you reboot you must be in Single Mouse mode to use the mouse at the Boot menu.

▶   **To configure the mouse to work at the Boot menu:**

1. Reboot the Mac and press the Option key during the reboot to open the Boot menu. The mouse will not respond at this point.

2. Select Intelligent Mouse mode and then select Single Mouse mode. The mouse will respond.

    Note: Mouse speed may be slow while in Single Mouse mode.

3. Once you are out of the Boot menu and have booted to the operating system, exit Single Mouse mode and switch back to Absolute Mouse mode for better mouse performance.

Chapter 7   User Management

In This Chapter

User Groups

The KSX II stores an internal list of all user and group names to determine access authorization and permissions. This information is stored internally in an encrypted format. There are several forms of authentication and this one is known as local authentication. All users have to be authenticated. If the KSX II is configured for LDAP/LDAPS or RADIUS, that authentication is processed first, followed by local authentication.

Every KSX II is delivered with three default user groups. These groups cannot be deleted:

User	Description
Admin	Users that are members of this group have full administrative privileges. The original, factory-default user is a member of this group and has the complete set of system privileges. In addition, the Admin user must be a member of the Admin group.
Unknown	This is the default group for users who are authenticated externally using LDAP/LDAPS or RADIUS or who are unknown to the system. If the external LDAP/LDAPS or RADIUS server does not identify a valid user group, the Unknown group is used. In addition, any newly created user is automatically put in this group until assigned to another group.
Individual Group	An individual group is essentially a "group" of one. That is, the specific user is in its own group, not affiliated with other real groups. Individual groups can be identified by the "@" in the Group Name. The individual group allows a user account to have the same rights as a group.

Up to 254 user groups can be created in the KSX II.

User Group List

User groups are used with local and remote authentication (via RADIUS or LDAP/LDAPS). It is a good idea to define user groups before creating individual users since, when you add a user, you must assign that user to an existing user group.

The User Group List page displays a list of all user groups, which can be sorted in ascending or descending order by clicking on the Group Name column heading. From the User Group List page, you can also add, modify, or delete user groups.

▶ **To list the user groups:**

- Choose User Management > User Group List. The User Group List page opens.

Relationship Between Users and Groups

Users belong to a group and groups have privileges. Organizing the various users of your KSX II into groups saves time by allowing you to manage permissions for all users in a group at once, instead of managing permissions on a user-by-user basis.

You may also choose not to associate specific users with groups. In this case, you can classify the user as "Individual."

Upon successful authentication, the device uses group information to determine the user's permissions, such as which server ports are accessible, whether rebooting the device is allowed, and other features.

Adding a New User Group

▶ **To add a new user group:**

1. Open the Group page by selecting User Management > Add New User Group or clicking the Add button from the User Group List page.

The Group page is organized into the following categories: Group, Permissions, Port Permissions, and IP ACL.

2. Type a descriptive name for the new user group into the Group Name field (up to 64 characters).

3. Set the permissions for the group. Select the checkboxes before the permissions you want to assign to all of the users belonging to this group. See *Permissions* (on page 116).

4. Set the port permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). See *Port Permissions* (on page 117).

5. Set the IP ACL. This feature limits access to the KSX II device by specifying IP addresses. It applies only to users belonging to a specific group, unlike the IP Access Control list feature that applies to all access attempts to the device (and takes priority). See *Group-Based IP ACL (Access Control List)* (on page 118).

6. Click OK.

Note: Several administrative functions are available within MPC and from the KSX II Local Console. These functions are available only to members of the default Admin group.

Note: Both IPv4 and IPv6 addresses are supported.

Setting Permissions for an Individual Group

▶ **To set permissions for an individual user group:**

1. Locate the group from among the groups listed. Individual groups can be identified by the @ in the Group Name.

2. Click the Group Name. The Group page opens.

3. Select the appropriate permissions.

4. Click OK.

Note: See Alternate RADIUS Authentication Settings for information on additional settings if you are using Alternate RADIUS Authentication.

Permissions

Important: Selecting the User Management checkbox allows the members of the group to change the permissions of all users, including their own. Carefully consider granting these permissions.

Permission	Description
Device Access While Under CC-SG Management	Allows users and user groups with this permission to directly access the KSX II using an IP address when Local Access is enabled for the device in CC-SG. The device can be accessed from the Local Console, Remote Console, MPC, VKC, and AKC. When a device is accessed directly while it is under CC-SG management, access and connection activity is logged on the KSX II. User authentication is performed based on KSX II authentication settings. *Note: The Admin user group has this permission by default.*
Device Settings	Network settings, date/time settings, port configuration (channel names, power associations), event management (SNMP, Syslog), virtual media file server setup
Diagnostics	Network interface status, network statistics, ping host, trace route to host, KSX II diagnostics
Maintenance	Backup and restore database, firmware upgrade, factory reset, reboot
Modem Access	Permission to use the modem to connect to the KSX II device
PC-Share	Simultaneous access to the same target by multiple users
Security	SSL certificate, security settings (VM Share, PC-Share), IP ACL
User	User and group management, remote

Permission	Description
Management	authentication (LDAP/LDAPS/RADIUS), login settings

Port Permissions

For each server port, you can specify the access type the group has, as well as the type of port access to the virtual media and the power control. Please note that the default setting for all permissions is Deny.

Port access	
Option	**Description**
Deny	Denied access completely
View	View the video (but not interact with) the connected target server
Control	Control the connected target server. Control must be assigned to the group if VM and power control access will also be granted.

VM access	
Option	**Description**
Deny	Virtual media permission is denied altogether for the port
Read-Only	Virtual media access is limited to read access only
Read-Write	Complete access (read, write) to virtual media

Power control access	
Option	**Description**
Deny	Deny power control to the target server
Access	Full permission to power control on a target server

For blade chassis, the port access permission will control access to the URLs that have been configured for that blade chassis.   The options are Deny or Control. In addition, each blade housed within the chassis has its own independent Port Permissions setting.

Group-Based IP ACL (Access Control List)

> Important: Exercise caution when using group-based IP access control. It is possible to be locked out of your KSX II if your IP address is within a range that has been denied access.

This feature limits access to the KSX II device by users in the selected group to specific IP addresses. This feature applies only to users belonging to a specific group, unlike the IP Access Control List feature that applies to all access attempts to the device, is processed first, and takes priority.

> Important: The IP address 127.0.0.1 is used by the KSX II Local Port and cannot be blocked.

Use the IP ACL section of the Group page to add, insert, replace, and delete IP access control rules on a group-level basis.
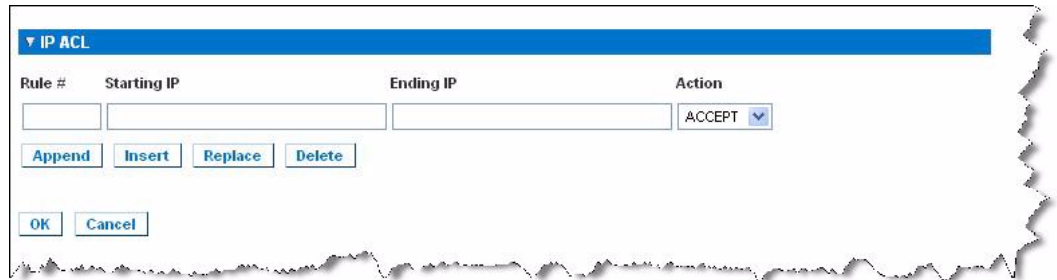
▶ **To add (append) rules:**

1. Type the starting IP address in the Starting IP field.

2. Type the ending IP address in the Ending IP field.

3. Choose the action from the available options:

   ▪ Accept - IP addresses set to Accept are allowed access to the KSX II device.

   ▪ Drop - IP addresses set to Drop are denied access to the KSX II device.

4. Click Append. The rule is added to the bottom of the rules list. Repeat steps 1 through 4 for each rule you want to enter.

▶ **To insert a rule:**

1. Enter a rule number (#). A rule number is required when using the Insert command.

2. Enter the Starting IP and Ending IP fields.

3. Choose the action from the Action drop-down list.

4. Click Insert. If the rule number you just typed equals an existing rule number, the new rule is placed ahead of the exiting rule and all rules are moved down in the list.

▶ **To replace a rule:**

1. Specify the rule number you want to replace.

2. Type the Starting IP and Ending IP fields.

3. Choose the Action from the drop-down list.

4. Click Replace. Your new rule replaces the original rule with the same rule number.

▶ **To delete a rule:**

1. Specify the rule number you want to delete.

2. Click Delete.

3. When prompted to confirm the deletion, click OK.

Important: ACL rules are evaluated in the order in which they are listed. For instance, in the example shown here, if the two ACL rules were reversed, Dominion would accept no communication at all.

Rule 1, Starting IP = 192.168.50.1, Ending IP = 192.168.55.255, Action = ACCEPT

Rule 2, Starting IP = 0.0.0.0, Ending IP = 255.255.255.255, Action = DROP

Tip: The rule numbers allow you to have more control over the order in which the rules are created.

Modifying an Existing User Group

Note: All permissions are enabled (and cannot be changed) for the Admin group.

▶ **To modify an existing user group:**

1. From the Group page, change the appropriate fields and set the appropriate permissions.

2. Set the Permissions for the group. Select the checkboxes before the permissions you want to assign to all of the users belonging to this group. See Setting Permissions.

3. Set the Port Permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). See **Setting Port Permissions**.

4. Set the IP ACL (optional). This feature limits access to the KSX II device by specifying IP addresses. See **Group-Based IP ACL (Access Control List)**.

5. Click OK.

▶ **To delete a user group:**

Important: If you delete a group with users in it, the users are automatically assigned to the <unknown> user group.

Tip: To determine the users belonging to a particular group, sort the User List by User Group.

1. Choose a group from among those listed by checking the checkbox to the left of the Group Name.

2. Click Delete.

3. When prompted to confirm the deletion, click OK.

Users

Users must be granted user names and passwords to gain access to the KSX II. This information is used to authenticate users attempting to access your KSX II.

User List

The User List page displays a list of all users including their user name, full name, and user group. The list can be sorted on any of the columns by clicking on the column name. From the User List page, you can also add, modify, or delete users.

▶ **To view the list of users:**

- Choose User Management > User List. The User List page opens.

Adding a New User

It is a good idea to define user groups before creating KSX II users because, when you add a user, you must assign that user to an existing user group. Refer to *Adding a New User Group* (on page 114) for more information.

From the User page, you can add new users, modify user information, and reactivate users that have been deactivated.

Note: A user name can be deactivated when the number of failed login attempts has exceeded the maximum login attempts set in the Security Settings page. Refer to **Security Settings** *(on page 189) for more information.*

▶ **To add a new user:**

1. Open the User page by choosing User Management > Add New User or clicking the Add button on the User List page.

2. Type a unique name in the Username field (up to 16 characters).

3. Type the person's full name in the Full Name field (up to 64 characters).

4. Type a password in the Password field and retype the password in the Confirm Password field (up to 64 characters).

5. If there is a dialback number, type it in the Dialback Number field. Dialback numbers cannot contain any of the following characters or the log on will fail when it is attempted:

   - " double quote
   - ' single quote
   - ; semicolon
   - $ dollar sign
   - & and sign
   - ½ pipe symbol

6. Choose the group from the User Group drop-down list. The list contains all groups you have created in addition to the system-supplied default groups (<Unknown> (default setting), Admin, Individual Group).

   If you do not want to associate this user with an existing User Group, select Individual Group from the drop-down list. For more information about permissions for an Individual Group, refer to *Setting Permissions for an Individual Group* (on page 115).

7. To activate the new user, select the Active checkbox. The default is activated (enabled).

8. Click OK.

Modifying an Existing User

▶ **To modify an existing user:**

1. Open the User List page by choosing User Management > User List.

2. Locate the user from among those listed on the User List page.

3. Click the user name. The User page opens.

4. On the User page, change the appropriate fields. See Adding a New User for information about how to get access the User page.

5. To delete a user, click Delete. You are prompted to confirm the deletion.

6. Click OK.

Logging a User Off (Force Logoff)

If you are an administrator, you are able to log off another locally authenticated user who is logged on to the KSX II.

▶ **To log off a user:**

1. Open the User List page by choosing User Management > User List or click the Connected User link in the left panel of the page.

2. Locate the user from among those listed on the User List page and select the checkbox next to their name.

3. Click the Force User Logoff button.

4. Click OK on the Logoff User dialog to forcefully log the user off.
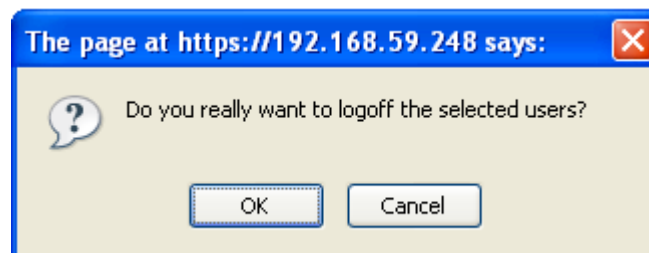
5. A confirmation message is displayed to indicate that the user was logged off. This message contains the date and time the log off occurred. Click OK to close the message.

Authentication Settings

Authentication is the process of verifying that a user is who he says he is. Once a user is authenticated, the user's group is used to determine his system and port permissions. The user's assigned privileges determine what type of access is allowed. This is called authorization.

When the KSX II is configured for remote authentication, the external authentication server is used primarily for the purposes of authentication, not authorization.

From the Authentication Settings page you can configure the type of authentication used for access to your KSX II.

Note: When remote authentication (LDAP/LDAPS or RADIUS) is selected, if the user is not found, the local authentication database will also be checked.

► **To configure authentication:**

1. Choose User Management > Authentication Settings. The Authentication Settings page opens.

2. Choose the option for the authentication protocol you want to use (Local Authentication, LDAP/LDAPS, or RADIUS). Choosing the LDAP option enables the remaining LDAP fields; selecting the RADIUS option enables the remaining RADIUS fields.

3. If you choose Local Authentication, proceed to step 6.

4. If you choose LDAP/LDAPS, read the section entitled **Implementing LDAP Remote Authentication** (see "**Implementing LDAP/LDAPS Remote Authentication**" on page 124) for information about completing the fields in the LDAP section of the Authentication Settings page.

5. If you choose RADIUS, read the section entitled **Implementing RADIUS Remote Authentication** (on page 128) for information about completing the fields in the RADIUS section of the Authentication Settings page.

6. Click OK to save.

► **To return to factory defaults:**

• Click the Reset to Defaults button.

Implementing LDAP/LDAPS Remote Authentication

Lightweight Directory Access Protocol (LDAP/LDAPS) is a networking protocol for querying and modifying directory services running over TCP/IP. A client starts an LDAP session by connecting to an LDAP/LDAPS server (through the default TCP port is 389). The client then sends operation requests to the server, and the server sends responses in turn.

Reminder: Microsoft® Active Directory® functions natively as an LDAP/LDAPS authentication server.

▶ **To use the LDAP authentication protocol:**

1. Click User Management > Authentication Settings to open the Authentication Settings page.

2. Select the LDAP radio button to enable the LDAP section of the page.

3. Click the ▶ LDAP icon to expand the LDAP section of the page.

    Server Configuration

4. In the Primary LDAP Server field, type the IP address or DNS name of your LDAP/LDAPS remote authentication server (up to 256 characters). When the Enable Secure LDAP option is selected and the Enable LDAPS Server Certificate Validation option is selected, the DNS name must be used to match the CN of LDAP server certificate.

5. In the Secondary LDAP Server field, type the IP address or DNS name of your backup LDAP/LDAPS server (up to 256 characters). When the Enable Secure LDAP option is selected, the DNS name must be used. Note that the remaining fields share the same settings with the Primary LDAP Server field. **Optional**

6. Type of External LDAP Server.

7. Select the external LDAP/LDAPS server. Choose from among the options available:

    ▪ Generic LDAP Server.

    ▪ Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.

8. Type the name of the Active Directory Domain if you selected Microsoft Active Directory. For example, *acme.com*. Consult your Active Directive Administrator for a specific domain name.

9. In the User Search DN field, enter the Distinguished Name of where in the LDAP database you want to begin searching for user information. Up to 64 characters can be used. An example base search value might be: `cn=Users,dc=raritan,dc=com`. Consult your authentication server administrator for the appropriate values to enter into these fields.

10. Enter the Distinguished Name of the Administrative User in the DN of Administrative User field (up to 64 characters). Complete this field if your LDAP server only allows administrators to search user information using the Administrative User role. Consult your authentication server administrator for the appropriate values to type into this field. An example DN of Administrative User value might be: `cn=Administrator,cn=Users,dc=testradius,dc=com`. **Optional**

11. In the Dialback Query String field, type the dialback query string. **Optional**

   If you are using Microsoft Active Directory, you must enter the following string: msRADIUSCallbackNumber. If you are not using Microsoft Active Directory, use the attribute string defined for that LDAP server.

   Note: This string is case sensitive.

12. If you entered a Distinguished Name for the Administrative User, you must enter the password that will be used to authenticate the Administrative User's DN against the remote authentication server. Enter the password in the Secret Phrase field and again in the Confirm Secret Phrase field (up to 128 characters).

LDAP/Secure LDAP

13. Select the Enable Secure LDAP checkbox if you would like to use SSL. This will enable the Enable LDAPS Server Certificate Validation checkbox. Secure Sockets Layer (SSL) is a cryptographic protocol that allows KSX II to communicate securely with the LDAP/LDAPS server.

14. The default Port is 389. Either use the standard LDAP TCP port or specify another port.

15. The default Secure LDAP Port is 636. Either use the default port or specify another port. This field is only used when the Enable Secure LDAP checkbox is selected.

16. Select the Enable LDAPS Server Certificate Validation checkbox to use the previously uploaded root CA certificate file to validate the certificate provided by the server. If you do not want to use the previously uploaded root CA certificate file, leave this checkbox deselected. Disabling this function is the equivalent of accepting a certificate that has been signed by an unknown certifying authority. This checkbox is only available when the Enable Secure LDAP checkbox has been enabled.

   Note: When the Enable LDAPS Server Certificate Validation option is selected, in addition to using the Root CA certificate for validation, the server hostname must match the common name provided in the server certificate.

17. If needed, upload the Root CA Certificate File. This field is enabled when the Enable Secure LDAP option is selected. Consult your authentication server administrator to get the CA certificate file in Base64 encoded X-509 format for the LDAP/LDAPS server. Use the Browse button to navigate to the certificate file. If you are replacing a certificate for the LDAP/LDAPS server with a new certificate, you must reboot the KSX II in order for the new certificate to take effect.

Test LDAP Server Access

18. The KSX II provides you with the ability to test the LDAP configuration from the Authentication Settings page due to the complexity sometimes encountered with successfully configuring the LDAP server and KSX II for remote authentication. To test the LDAP configuration, enter the login name and password in the "Login for testing" field and the "Password for testing" field respectively. This is the username and password you entered to access the KSX II and that the LDAP server will use to authenticate you. Click Test.

19. Once the test is completed, a message will be displayed that lets you know the test was successful or, if the test failed, a detailed error message will be displayed. It will display successful result or detail error message in failure case. It also can display group information retrieved from remote LDAP server for the test user in case of success.

Returning User Group Information from Active Directory Server

The KSX II supports user authentication to Active Directory® (AD) without requiring that users be defined locally on the KSX II. This allows Active Directory user accounts and passwords to be maintained exclusively on the AD server. Authorization and AD user privileges are controlled and administered through the standard KSX II policies and user group privileges that are applied locally to AD user groups.

IMPORTANT: If you are an existing Raritan, Inc. customer, and have already configured the Active Directory server by changing the AD schema, the KSX II still supports this configuration and you do not need to perform the following operations. See Updating the LDAP Schema for information about updating the AD LDAP/LDAPS schema.

▶ **To enable your AD server on the KSX II:**

1. Using the KSX II, create special groups and assign proper permissions and privileges to these groups. For example, create groups such as KVM_Admin and KVM_Operator.

2. On your Active Directory server, create new groups with the same group names as in the previous step.

3. On your AD server, assign the KSX II users to the groups created in step 2.

4. From the KSX II, enable and configure your AD server properly. See Implementing LDAP/LDAPS Remote Authentication.

Important Notes:

- Group Name is case sensitive.

- The KSX II provides the following default groups that cannot be changed or deleted: Admin and <Unknown>. Verify that your Active Directory server does not use the same group names.

- If the group information returned from the Active Directory server does not match a KSX II group configuration, the KSX II automatically assigns the group of <Unknown> to users who authenticate successfully.

- If you use a dialback number, you must enter the following case-sensitive string: *msRADIUSCallbackNumber.*

- Based on recommendations from Microsoft, Global Groups with user accounts should be used, not Domain Local Groups.

Implementing RADIUS Remote Authentication

Remote Authentication Dial-in User Service (RADIUS) is an AAA (authentication, authorization, and accounting) protocol for network access applications.

▶ **To use the RADIUS authentication protocol:**

1. Click User Management > Authentication Settings to open the Authentication Settings page.

2. Click the RADIUS radio button to enable the RADIUS section of the page.

3. Click the ▸ **RADIUS** icon to expand the RADIUS section of the page.

4. In the Primary Radius Server and Secondary Radius Server fields, type the IP address of your primary and optional secondary remote authentication servers, respectively (up to 256 characters).

5. In the Shared Secret fields, type the server secret used for authentication (up to 128 characters).

   The shared secret is a character string that must be known by both the KSX II and the RADIUS server to allow them to communicate securely. It is essentially a password.

6. The Authentication Port default is port is 1812 but can be changed as required.

7. The Accounting Port default port is 1813 but can be changed as required.

8. The Timeout is recorded in seconds and default timeout is 1 second, but can be changed as required.

   The timeout is the length of time the KSX II waits for a response from the RADIUS server before sending another authentication request.

9. The default number of retries is 3 Retries.

   This is the number of times the KSX II will send an authentication request to the RADIUS server.

10. Choose the Global Authentication Type from among the options in the drop-down list:

   ▪ PAP - With PAP, passwords are sent as plain text. PAP is not interactive. The user name and password are sent as one data package once a connection is established, rather than the server sending a login prompt and waiting for a response.

- CHAP - With CHAP, authentication can be requested by the server at any time. CHAP provides more security than PAP.

Returning User Group Information via RADIUS

When a RADIUS authentication attempt succeeds, the KSX II determines the permissions for a given user based on the permissions of the user's group.

Your remote RADIUS server can provide these user group names by returning an attribute, implemented as a RADIUS FILTER-ID. The FILTER-ID should be formatted as follows: Raritan:G{*GROUP_NAME*} where *GROUP_NAME* is a string denoting the name of the group to which the user belongs.

```
Raritan:G{GROUP_NAME}:D{Dial Back Number}
```

where GROUP_NAME is a string denoting the name of the group to which the user belongs and Dial Back Number is the number associated with the user account that the KSX II modem will use to dial back to the user account.

RADIUS Communication Exchange Specifications

The KSX II sends the following RADIUS attributes to your RADIUS server:

Attribute	Data
Log in	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-IP-Address (4)	The IP address for the KSX II.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
User-Password(2)	The encrypted password.
Accounting-Request(4)	
Acct-Status (40)	Start(1) - Starts the accounting.
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.
NAS-IP-Address (4)	The IP address for the KSX II.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.

Attribute	Data
Log out	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - Stops the accounting
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.
NAS-IP-Address (4)	The IP address for the KSX II.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.

User Authentication Process

Remote authentication follows the process specified in the flowchart below:
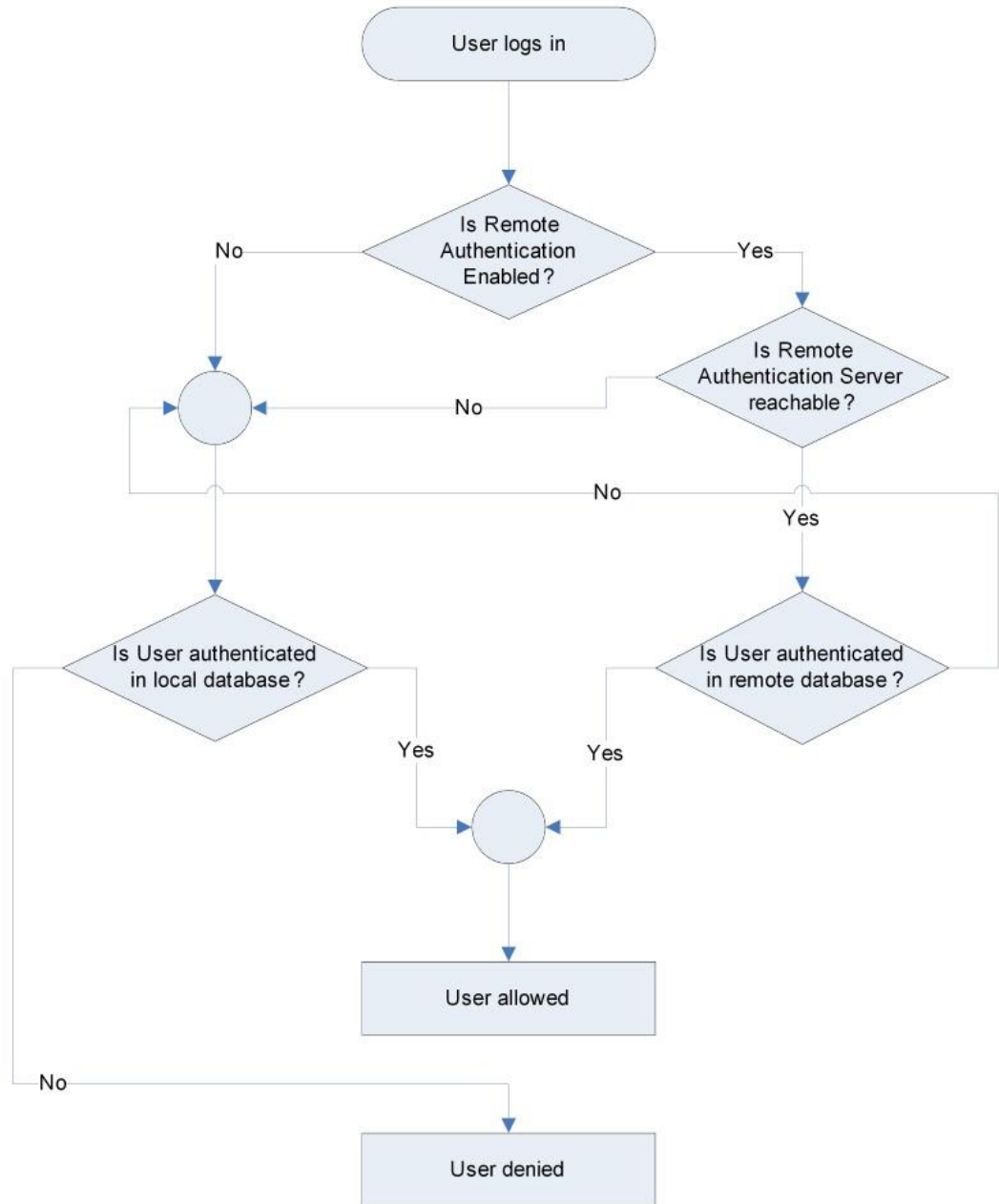
Changing a Password

▶ **To change your password:**

1. Choose User Management > Change Password. The Change Password page opens.

2. Type your current password in the Old Password field.

3. Type a new password in the New Password field. Retype the new password in the Confirm New Password field. Passwords can be up to 64 characters in length and can consist of English alphanumeric characters and special characters.

4. Click OK.

5. You will receive confirmation that the password was successfully changed. Click OK.

Note: If strong passwords are in use, this page displays information about the format required for the passwords. For more information about passwords and strong passwords, see **Strong Passwords** *(on page 191).*

Home > User Management > Change Password

Change Password

Old Password

New Password

Confirm New Password

OK   Cancel

Chapter 8   Device Management

In This Chapter

Network Settings

Use the Network Settings page to customize the network configuration (for example, the IP address, discovery port, and LAN interface parameters) for your KSX II.

There are two options available to set up your IP configuration:

- None (default) - This is the recommended option (static IP). Since the KSX II is part of your network infrastructure, you most likely do not want its IP address to change frequently. This option allows you to set the network parameters.

- DHCP - With this option, the IP address is automatically assigned by a DHCP server.

▶ **To change the network configuration:**

1. Choose Device Settings > Network. The Network Settings page opens.

2. Update the Network Basic Settings. See Network Basic Settings.

3. Update the LAN Interface Settings. See LAN Interface Settings.

4. Click OK to set these configurations. If your changes require rebooting the device, a reboot message appears.

▶ **To reset to factory defaults:**

- Click Reset to Defaults.

Note: Both IPv4 and IPv6 addresses are supported.

Network Basic Settings

These procedures describe how to assign an IP address on the Network Settings page. For complete information about all of the fields and the operation of this page, see **Network Settings**.

▶ **To assign an IP address:**

1. Choose Device Settings > Network. The Network Settings page opens.

2. Specify a meaningful Device Name for your KSX II device. Up to 32 alphanumeric characters using valid special characters and no spaces.

3. In the IPv4 section, enter or select the appropriate IPv4-specific network settings:

   a. Enter the IP Address if needed. The default IP address is 192.168.0.192.

   b. Enter the Subnet Mask. The default subnet mask is 255.255.255.0.

   c. Enter the Default Gateway if None is selected from the IP Auto Configuration drop-down.

   d. Enter the Preferred DHCP Host Name if DHCP is selected from the IP Auto Configuration drop-down.

   e. Select the IP Auto Configuration. The following options are available:

   ▪ None (Static IP) - This option requires that you manually specify the network parameters.

     This is the recommended option because the KSX II is an infrastructure device and its IP address should not change.

   ▪ DHCP - Dynamic Host Configuration Protocol is used by networked computers (clients) to obtain unique IP addresses and other parameters from a DHCP server.

     With this option, network parameters are assigned by the DHCP server. If DHCP is used, enter the Preferred host name (DHCP only). Up to 63 characters.

4. If IPv6 is to be used, enter or select the appropriate IPv6-specific network settings in the IPv6 section:

   a. Select the IPv6 checkbox to activate the fields in the section.

   b. Enter a Global/Unique IP Address. This is the IP address assigned to the KSX II.

   c. Enter the Prefix Length. This is the number of bits used in the IPv6 address.

    d.   Enter the Gateway IP Address.

    e.   Link-Local IP Address. This address is automatically assigned to the device. It is used for neighbor discovery or when no routers are present. **Read-Only**

    f.   Zone ID. This identifies the device with which the address is associated. **Read-Only**

    g.   Select the IP Auto Configuration. The following options are available:

- None - Use this option if you do not want an auto IP configuration and prefer to set the IP address yourself (static IP). This is the default and recommended option.

  If None is selected for the IP auto configuration, the following Network Basic Settings fields are enabled: Global/Unique IP Address, Prefix Length, and Gateway IP Address allowing you to manually set the IP configuration.

- Router Discovery - Use this option to automatically assign IPv6 addresses that have Global or Unique Local significance beyond that of the Link Local, which only applies to a directly connected subnet.

5. Select Obtain DNS Server Address Automatically if DHCP is selected and Obtain DNS Server Address is enabled. When Obtain DNS Server Address Automatically, the DNS information provided by the DHCP server will be used.

6. If Use the Following DNS Server Addresses is selected, regardless of whether DHCP is selected or not, the addresses entered in this section will be used to connect to the DNS server.

   Enter the following information if the Following DNS Server Addresses option is selected. These addresses are the primary and secondary DNS addresses that will be used if the primary DNS server connection is lost due to an outage.

   a.   Primary DNS Server IP Address

   b.   Secondary DNS Server IP Address

7. When finished, click OK. Your KSX II device is now network accessible.

See *LAN Interface Settings* (on page 138) for information in configuring this section of the Network Settings page.

Note: In some environments, the default LAN Interface Speed & Duplex setting Autodetect (autonegotiator) does not properly set the network parameters, which results in network issues. In these instances, setting the KSX II LAN Interface Speed & Duplex field to 100 Mbps/Full Duplex (or whatever option is appropriate to your network) addresses the issue. See the **Network Settings** *(on page 135) page for more information.*

LAN Interface Settings

1. The current parameter settings are identified in the Current LAN interface parameters field.

2. Choose the LAN Interface Speed & Duplex from the following options:

- Autodetect (default option)
- 10 Mbps/Half - Both LEDs blink
- 10 Mbps/Full - Both LEDs blink
- 100 Mbps/Half - Yellow LED blinks
- 100 Mbps/Full - Yellow LED blinks
- 1000 Mbps/Full (gigabit) - Green LED blinks
- Half-duplex provides for communication in both directions, but only one direction at a time (not simultaneously).
- Full-duplex allows communication in both directions simultaneously.

Note: Occasionally there are problems running at 10 Mbps in either half or full duplex. If you are experiencing problems, try another speed and duplex setting.

See **Network Speed Settings** (on page 289) for more information.

3. Select the Enable Automatic Failover checkbox to allow the KSX II to automatically recover its network connection using a second network port if the active network port fails.

Note: Because a failover port is not activated until after a failover has actually occurred, Raritan recommends that you not monitor the port or monitor it only after a failover occurs.

When this option is enabled, the following two fields are used:

- Ping Interval (seconds) - Ping interval determines how often the KSX II checks the status of the network path to the designated gateway. The default ping interval is 30 seconds.
- Timeout (seconds) - Timeout determines how long a designated gateway remains unreachable via the network connection before a fail over occurs.

Note: The ping interval and timeout can be configured to best meet the local network conditions. The timeout should be set to allow for at least two or more ping requests to be transmitted and responses returned. For example, if a high rate of failover is observed due to high network utilization, the timeout should be extended to 3 or 4 times the ping interval.

4. Select the Bandwidth.
5. Click OK to apply the LAN settings.

Device Services

The Device Services page allows you to configure the following functions:

- Enabling Telnet
- Enabling SSH access
- Configuring HTTP and HTTPs port settings
- Enabling Serial Console Access
- Configuring the discovery port access
- Enabling direct port access
- Enabling the AKC Download Server Certificate Validation feature if you are using AKC

Enabling Telnet

If you wish to use Telnet to access the KSX II, first access the KSX II from the CLI or a browser.

▶ **To enable Telnet:**

1. Select Device Settings > Device Services and then select the Enable TELNET Access checkbox.

2. Enter the Telnet port.

3. Click OK.

Once Telnet access is enabled, you can use it to access the KSX II and set up the remaining parameters.

Enabling SSH

Enable SSH access to allow administrators to access the KSX II via the SSH v2 application.

▶ **To enable SSH access:**

1. Choose Device Settings > Device Services. The Device Service Settings page appears.

2. Select Enable SSH Access.

3. Enter the SSH Port information. The standard SSH TCP port number is 22 but the port number can be changed to provide a higher level of security operations.

4. Click OK.

HTTP and HTTPS Port Settings

You are able to configure HTTP and/or HTTPS ports used by the KSX II. For example, if you are using the default HTTP port 80 for another purpose, changing the port will ensure the KSX II does not attempt to use it.

▶ **To change the HTTP and/or HTTPS port settings:**

1. Choose Device Settings > Device Services. The Device Service Settings page appears.

2. Enter the new ports in the HTTP Port and/or HTTPS Port fields.

3. Click OK.

Entering the Discovery Port

The KSX II discovery occurs over a single, configurable TCP Port. The default is Port 5000, but you can configure it to use any TCP port except 80 and 443. To access the KSX II from beyond a firewall, your firewall settings must enable two-way communication through the default Port 5000 or a non-default port configured here.

▶ **To enable the discovery port:**

1. Choose Device Settings > Device Services. The Device Service Settings page appears.

2. Enter the Discovery Port.

3. Click OK.

Enabling Serial Console Access

▶ **To enable serial console access:**

1. Choose Device Settings > Device Services. The Device Service Settings page appears.

2. Select Enable Serial Console Access.

3. Select the baud rate of the device.

4. Click OK.

Enabling Direct Port Access via URL

Direct port access allows users to bypass having to use the device's Login dialog and Port Access page. This feature also provides the ability to enter a username and password directly and proceed to the target if the username and password is not contained in the URL.

Note: You are also able to configure direct port access via URL. See **Configuring Direct Port Access via Telnet, IP Address or SSH** *(on page 34).*

The following is important URL information regarding direct port access:

If you are using VKC and direct port access:

- https://IPaddress/dpa.asp?username=username&password=password&port=port number

If you are using AKC and direct port access:

- https://IPaddress/dpa.asp?username=username&password=password&port=port number&client=akc

Where:

- Username and password are optional. If they are not provided, a login dialog will be displayed and, after being authenticated, the user will be directly connected to the target.

- The port may be a port number or port name. If you are using a port name, the name must be unique or an error is reported. If the port is omitted altogether, an error is reported.

- For blade chassis, the port is designated <port number>'-'<slot number>. For example, 1-2 for blade chassis connected to port 1, slot 2.

- Client=akc is optional unless you are using the AKC client. If client=akc is not included, VKC is used as the client.

▶ **To enable direct port access:**

1. Choose Device Settings > Device Services. The Device Service Settings page appears.

2. Select Enable Direct Port Access via URL if you would like users to have direct access to a target via the Dominion device by passing in the necessary parameters in the URL.

❈ Raritan.

3. Click OK.

No.	Name	IP Address	SSH Port	Telnet Port
9	Serial Port 1			
10	Serial Port 2			
11	Serial Port 3			
12	Serial Port 4			
13	Serial Port 5			
14	Serial Port 6			
15	Serial Port 7			
16	Serial Port 8			

Direct Port Access

OK   Reset To Defaults   Cancel

Configuring Direct Port Access via Telnet, IP Address or SSH

The information in this topic is specific to enabling direct port access for serial targets. Use the Enable Direct Port Access via URL option on the Device Services page to enable direct port access for a KVM/serial port connect to the KSX II. See *Enabling Direct Port Access via URL* (on page 142).

▶   **To configure direct port access:**

1. Choose Device Settings > Device Services. The Device Service Settings page opens.

2. Type the IP address and ports used for SSH and Telnet in the appropriate fields for each serial target.

    Note that leaving all three fields blank will disable direct port access for the serial target. To enable direct port access, you must do one of the following:

    ▪   Enable global Telnet or SSH access.

    ▪   Input a valid IP address or TCP port in at least one of the three fields.

    Important: It is not recommended that more than one of these fields is populated.

    Below are examples of Telnet and IP:

    ▪   Direct Port access via IP alias address:

        Configure the IP alias address 192.168.1.59 for a serial target. Once this is done, connection to the target through Telnet can be done using "telnet 192.168.1.59".

    ▪   Direct Port access via Telnet port:

Configure the Telnet TCP Port as "7770". Once this is done, connection to the target can be done using "telnet <KSX II device IP address> 7770".

- Direct Port Access via SSH Port:

Configure the SSH TCP port as "7888". Once this is done, connection to the target can be done by using "ssh –l <login> <KSX II device IP address> -p 7888".

3. Click OK to save this information.

Direct Port Access

No.	Name	IP Address	SSH Port	Telnet Port
9	Serial Port 1			
10	Serial Port 2			
11	Serial Port 3			
12	Serial Port 4			
13	Serial Port 5			
14	Serial Port 6			
15	Serial Port 7			
16	Serial Port 8			

OK   Reset To Defaults   Cancel

Once you have created the direct port access, it can be connected in a client application such as PuTTY. Following is an example of how the direct port access information would appear in PuTTY. Note that PuTTY is not the only client application that can be used. It is used here for sample purposes only.

Enabling the AKC Download Server Certificate Validation

If you are using the AKC client, you can choose to use the Enable AKC Download Server Certificate Validation feature or opt not to use this feature.

Option 1: Do Not Enable AKC Download Server Certificate Validation (default setting)

If you do not enable AKC Download Server Certificate Validation, all Dominion device users and CC-SG Bookmark and Access Client users must:

- Ensure the cookies from the IP address of the device that is being accessed are not currently being blocked.

- Windows Vista, Windows 7 and Windows 2008 server users should ensure that the IP address of the device being accessed is included in their browser's Trusted Sites Zone and that Protected Mode is not on when accessing the device.

Option 2: Enable AKC Download Server Certificate Validation

If you do enable AKC Download Server Certificate Validation:

- Administrators must upload a valid certificate to the device or generate a self-signed certificate on the device. The certificate must have a valid host designation.

- Each user must add the CA certificate (or a copy of self-signed certificate) to the Trusted Root CA store in their browser.

▶ **To install the self-signed certificate when using Windows Vista® operating system and Windows 7® operating system:**

1. Include the KSX II IP address in the Trusted Site zone and ensure 'Protected Mode' is off.

2. Launch Internet Explorer® using the KSX II IP address as the URL. A Certificate Error message will be displayed.

3. Select View Certificates.

4. On the General tab, click Install Certificate. The certificate is then installed in the Trusted Root Certification Authorities store.

5. After the certificate is installed, the KSX II IP address can be removed from the Trusted Site zone.

▶ **To enable AKC download server certificate validation:**

1. Choose Device Settings > Device Services. The Device Service Settings page appears.

2. Select the Enable AKC Download Server Certificate Validation checkbox or you can leave the feature disabled (default).

3. Click OK.

Configuring Modem Settings

▶ **To configure modem settings:**

1. Click Device Settings > Modem Settings to open the Modem Settings page.

2. Check Enable Modem, if needed.

3. Enter the PPP server IP address. The internet address assigned to the KSX II when a connection is established via dial-up. Required.

4. Enter the PPP client IP address. The internet address the KSX II assigns to remove the client when a connection is established via dial-up. **Required**

   Note: The PPP server IP address and PPP Client IP address must be different and cannot conflict with the network addresses used by the server or the client.

5. Check Enable Modem Dialback, if needed.

   Note: If dial-back is enabled, each user accessing the KSX II via modem must have a call-back number defined in their profile. Otherwise, dial-up will reject the call for that user.

6. Click OK to commit your changes or click Reset to Defaults to return the settings to their defaults.

Configuring Date/Time Settings

Use the Date/Time Settings page to specify the date and time for the KSX II. There are two ways to do this:

- Manually set the date and time.
- Synchronize the date and time with a Network Time Protocol (NTP) server.

▶ **To set the date and time:**

1. Choose Device Settings > Date/Time. The Date/Time Settings page opens.

2. Choose your time zone from the Time Zone drop-down list.

3. To adjust for daylight savings time, check the "Adjust for daylight savings time" checkbox.

4. Choose the method you would like to use to set the date and time:

   - User Specified Time - Choose this option to input the date and time manually.

     For the User Specified Time option, enter the date and time. For the time, use the hh:mm format (using a 24-hour clock).

   - Synchronize with NTP Server - Choose this option to synchronize the date and time with the Network Time Protocol (NTP) Server.

5. For the Synchronize with NTP Server option:

   a. Enter the IP address of the Primary Time server.

   b. Enter the IP address of the Secondary Time server. **Optional**

6. Click OK.

Event Management

The KSX II Event Management feature allows you enable and disable the distribution of system events to SNMP Managers, the Syslog and the audit log. These events are categorized, and for each event you can determine whether you want the event sent to one or several destinations.

149

Configuring Event Management Settings

SNMP Configuration

Simple Network Management Protocol (SNMP) is a protocol governing network management and the monitoring of network devices and their functions. KSX II offers SNMP Agent support through Event Management.

▶ **To configure SNMP (enable SNMP logging):**

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page opens.

2. Choose the Enable SNMP Logging option. This enables the remaining SNMP fields.

3. In the Name, Contact, and Location fields, type the SNMP agent's name (that is, the device's name) as it appears in the KSX II Console interface, a contact name related to this device, and where the Dominion device is physically located, respectively.

4. Type the Agent Community String (the device's string). An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. The SNMP device or agent may belong to more than one SNMP community.

5. Specify whether the community is Read-Only or Read-Write using the Type drop-down list.

6. Configure up to five SNMP managers by specifying their Destination IP, Port #, and Community.

7. Click the "Click here to view the Dominion- SNMP MIB" link to access the SNMP Management Information Base.

8. Click OK.

Syslog Configuration

▶ **To configure the Syslog (enable Syslog forwarding):**

1. Choose the Enable Syslog Forwarding option to log the device's messages to a remote Syslog server.

2. Type the IP Address of your Syslog server in the IP Address field.

3. Click OK.

▶ **To reset to factory defaults:**

*   Click the Reset To Defaults button.

Note: Both IPv4 and IPv6 addresses are supported.

Note: IPv6 addresses cannot exceed 80 characters in length for the host name.

Configuring Event Management - Destinations

System events, if enabled, can generate SNMP notification events (traps), or can be logged to syslog or audit log. Use the Event Management - Destinations page to select which system events to track and where to send this information.

Note: SNMP traps will only be generated if the SNMP Logging Enabled option is checked; Syslog events will only be generated if the Enable Syslog Forwarding option is checked. Both of these options are in the Event Management - Settings page. See **Event Management - Settings** *(see "***Configuring Event Management Settings***" on page 150).*

▶ **To select events and their destinations:**

1. Choose Device Settings > Event Management - Destinations. The Event Management - Destinations page opens.

System events are categorized by Device Operation, Device Management, Security, User Activity, and User Group Administration.

2. Check the checkboxes for those event line items you want to enable or disable, and where you want to send the information.

   Tip: Enable or disable entire categories by checking or clearing the category line checkboxes, respectively.

3. Click OK.

▶ **To reset to factory defaults:**

   ▪ Click the Reset To Defaults button.

SNMP Trap Configuration

SNMP provides the ability to send traps, or notifications, to advise an administrator when one or more conditions have been met. The following table lists the KSX II SNMP traps:

Trap name	Description
cimConnected	A CIM is plugged into to the KSX II port.
cimDisconnected	A CIM is either unplugged from the KSX II port or powered-off.
cimUpdateCompleted	CIM firmware update process completed.
cimUpdateStarted	CIM firmware update process started.
configBackup	The device configuration has been backed up.
configRestore	The device configuration has been restored.
deviceUpdateFailed	Device update has failed.
deviceUpgradeCompleted	The KSX II has completed update via an RFP file.
deviceUpgradeStarted	The KSX II has begun update via an RFP file.
ethernetFailover	An Ethernet failover was detected and restored on a new Ethernet interface.
factoryReset	The device has been reset to factory defaults.
firmwareFileDiscarded	Firmware file was discarded.
firmwareUpdateFailed	Firmware update failed.
firmwareValidationFailed	Firmware validation failed.
groupAdded	A group has been added to the KSX II system.
groupDeleted	A group has been deleted from the system.
groupModified	A group has been modified.
ipConflictDetected	An IP Address conflict was detected.
ipConflictResolved	An IP Address conflict was resolved.
networkFailure	An Ethernet interface of the product can no longer communicate over the

Trap name	Description
	network.
networkParameterChanged	A change has been made to the network parameters.
passwordSettingsChanged	Strong password settings have changed.
portConnect	A previously authenticated user has begun a KVM session.
portConnectionDenied	A connection to the target port was denied.
portDisconnect	A user engaging in a KVM session closes the session properly.
portStatusChange	The port has become unavailable.
powerNotification	The power outlet status notification: 1=Active, 0=Inactive.
powerOutletNotification	Power strip device outlet status notification.
rebootCompleted	The KSX II has completed its reboot.
rebootStarted	The KSX II has begun to reboot, either through cycling power to the system or by a warm reboot from the OS.
securityViolation	Security violation.
startCCManagement	The device has been put under CommandCenter Management.
securityBannerChanged	The security banner has changed.
securityBannerAction	User Acceptance/Rejection of Security Banner.
setDateTime	The device time and date have been set.
setPIPSMode	FIPS Mode status has been changed on the device.
bladeChassisCommError	A communications error with the blade chassis device connected to this port was detected.
stopCCManagement	The device has been removed from CommandCenter Management.
sxPortAlert	Logs keywords and sends out an event.
userAdded	A user has been added to the system.

Trap name	Description
userAuthenticationFailure	A user attempted to log in without a correct username and/or password.
userConnectionLost	A user with an active session has experienced an abnormal session termination.
userDeleted	A user account has been deleted.
userLogin	A user has successfully logged into the KSX II and has been authenticated.
userLogout	A user has successfully logged out of the KSX II properly.
userModified	A user account has been modified.
userPasswordChanged	This event is triggered if the password of any user of the device is modified.
userSessionTimeout	A user with an active session has experienced a session termination due to timeout.
vmImageConnected	User attempted to mount either a device or image on the target using Virtual Media. For every attempt on device/image mapping (mounting) this event is generated.
vmImageDisconnected	User attempted to unmount a device or image on the target using Virtual Media.

Configuring Ports

The Port Configuration page displays a list of the KSX II ports. Ports connected to KVM target servers (blades and standard servers) and rack PDUs (power strips) are displayed in blue and can be edited. For ports with no CIM connected or with a blank CIM name, a default port name of Dominion_KSX2_Port# is assigned, where Port# is the number of the KSX II physical port.

▶ **To access a port configuration:**

1. Choose Device Settings > Port Configuration. The Port Configuration Page opens.

   This page is initially displayed in port number order, but can be sorted on any of the fields by clicking on the column heading.

   ▪ Port Number - Numbered from 1 to the total number of ports available for the KSX II device.

- Port Name - The name assigned to the port. A port name displayed in black indicates that you cannot change the name and that the port cannot be edited; port names displayed in blue can be edited.

Note: Do not use apostrophes for the Port (CIM) Name.

- Port Type

Port type	Description
DCIM	Dominion CIM
Not Available	No CIM connected
PCIM	Paragon CIM
PowerStrip (rack PDU)	Power strip connected
VM	Virtual media CIM (D2CIM-VUSB and D2CIM-DVUSB)
Blade Chassis	Blade chassis and the blades associated with that chassis (displayed in a hierarchical order)

2. Click the Port Name for the port you want to edit.

- For KVM ports, the Port page for KVM and blade chassis ports is opened.

- For rack PDUs, the Port page for rack PDUs (power strips) is opened. From this page, you can name the rack PDUs and their outlets.

▪ For serial ports, the Port page for serial ports is opened.

Port Configuration

▲ No.	Name	Type
1	KX-local	Not Available
2	Dominion_KSX2_Port2	Not Available
3	KX8-Local	Not Available
4	Dominion_KSX2_Port4	Not Available
5	Blade_Chassis_Port3	Not Available
6	Dominion_KSX2_Port6	Not Available
7	Dominion_KSX2_Port7	Not Available
8	Dominion_KSX2_Port8	Not Available
9	Serial Port 1	Serial
10	Serial Port 2	Serial
11	Serial Port 3	Serial
12	Serial Port 4	Serial
13	Serial Port 5	Serial
14	Serial Port 6	Serial
15	Serial Port 7	Serial
16	Serial Port 8	Serial
17	Power Port 1	PowerStrip
18	Power Port 2	PowerStrip

157

Power Control

Power control is configured on the Port page. The Port page opens when you select a port that is connected to a target server from the Port Configuration page.

From the Port page, you can make power associations and change the port name to something more descriptive.

A server can have up to four (4) power associates and you can associate a different rack PDU (power strip) with each. From this page, you can define those associations so that you can power on, power off, and power cycle the server from the Port page.

See **E. Power Strip** (see "**E. Rack PDU (Power Strip)**" on page 28) of this guide for information on the physical connections between the KSX II and Dominion PX.

Port 1

Type:
PCIM
Name:
KX-local

Power Association

Power Strip Name   Outlet Name
None   ---
None   ---
None   ---
None   ---

Target Settings

☐ 720x400 Compensation

☐ Use international keyboard for scan code set 3

OK   Cancel

Assigning a Name to the PX

The Port page opens when you select a port on the Port Configuration page. The port appears on this page when connected to a Raritan remote rack PDU (power strip). The Type and the Name fields are prepopulated.

Use this page to name the rack PDU and its outlets; all names can be up to 32 alphanumeric characters and can include special characters.

Note: When a rack PDU is associated to a target server (port), the outlet name is replaced by the target server name (even if you assigned another name to the outlet).

Note: CommandCenter Service Gateway does not recognize rack PDU names containing spaces.

▶ **To name the rack PDU (and outlets):**

1. Change the Name of the rack PDU to something you will remember.

2. Change the (Outlet) Name, if desired. (Outlet names default to Outlet #.)

3. Click OK.

Associating KVM and Serial Target Servers to Outlets (Port Page)

A server can have up to four power plugs and you can associate a different rack PDU (power strip) with each. From the Port page, you can define those associations so that you can power on, power off, and power cycle the server.

The KVM and serial Port pages are different from each other with the exception of the Name and Port Association sections. Since the Power Association sections are the same, the steps below apply to both KVM and serial target servers.

▶ **To make power associations (associate rack PDU outlets to target servers):**

Note: When a rack PDU is associated to a target server (port), the outlet name is replaced by the target server name (even if you assigned another name to the outlet).

1. Choose the rack PDU from the Power Strip Name drop-down list.

2. For that rack PDU, choose the outlet from the Outlet Name drop-down list.

3. Repeat steps 1 and 2 for all desired power associations.

4. Click OK. A confirmation message is displayed.

▶ **To remove a rack PDU association:**

1. Select the appropriate rack PDU from the Power Strip Name drop-down list.

2. For that rack PDU, select the appropriate outlet from the Outlet Name drop-down list.

3. From the Outlet Name drop-down list, select None.

4. Click OK. The rack PDU/outlet association is removed and a confirmation message is displayed.

Target Settings

▶ **To define target settings:**

1. In the Target Settings section, select 720x400 Compensation if you are experiencing display issues when the target is using this resolution.

2. Select 'Use international keyboard for scan code set 3' if connecting to the target with a DCIM-PS2 and require the use of scan code set 3 with an international keyboard.

Configuring Blade Chassis

In addition to standard servers and rack PDUs (power strips), you can control blade chassis that are plugged into a Dominion device port. Up to eight blade chassis can be managed at a given time.

As with standard servers, blade chassis are autodetected once they are connected. When a blade server chassis is detected, a default name is assigned to it and it is displayed on the Port Access page along with standard target servers and rack PDUs (see Port Access Page). The blade chassis is displayed in an expandable, hierarchical list on the Port Access page, with the blade chassis at the root of the hierarchy and the individual blades labeled and displayed below the root. Use the Expand Arrow icon next to the root chassis to display the individual blades.

Note: To view the blade chassis in a hierarchal order, blade-chassis subtypes must be configured for the blade server chassis.

With the exception of HP® blade chassis, generic, IBM®, and Dell® blade chassis are configured on the Port page. The port connected to the blade chassis must be configured with the blade chassis model. The specific information you are able to configure for a blade server will depend on the brand of blade server you are working with. For specific information on each of these supported blade chassis, see their corresponding topics in this section of the help.

The following blade chassis are supported:

- IBM BladeCenter® Models E and H
- Dell PowerEdge® 1855, 1955 and M1000e

A Generic option allows you to configure a blade chassis that is not included in the above list. HP BladeSystem c3000 and c7000 are supported via individual connections from the Dominion device to each blade. The ports are 'grouped' together into a chassis representation using the Port Group Management feature.

Note: Dell PowerEdge 1855/1955 blades also provide the ability to connect from each individual blade to a port on the Dominion device. When connected in that manner, they can also be grouped to create blade server groups.

Two modes of operation are provided for blade chassis: manual configuration and auto-discovery, depending on the blade chassis capabilities. If a blade chassis is configured for auto-discovery, the Dominion device tracks and updates the following:

- When a new blade server is added to the chassis.
- When an existing blade server is removed from the chassis.

Note: In the case of IBM Blade Center Models E and H, the KSX II only supports auto-discovery for AMM[1] as the acting primary management module.

The use of hot key sequences to switch KVM access to a blade chassis is also supported. For blade chassis that allow users to select a hot key sequence, those options will be provided on the Port Configuration page. For blade chassis that come with predefined hot key sequences, those sequences will be prepopulated on the Port Configuration page once the blade chassis is selected. For example, the default hot key sequence to switch KVM access to an IBM BladeCenter H is NumLock + NumLock + SlotNumber, so this hot key sequence is applied by default when IBM BladeCenter H is selected during the configuration. See your blade chassis documentation for hot key sequence information.

You are able to configure the connection to a blade chassis web browser interface if one is available. At the chassis level, up to four links can be defined. The first link is reserved for connection to the blade chassis administrative module GUI. For example, this link may be used by technical support to quickly verify a chassis configuration.

Blade chassis can be managed from the Virtual KVM Client (VKC), the Active KVM Client (AKC), Raritan's Multi-Platform Client (MPC), and CC-SG. Managing blade severs via VKC, AKC and MPC is the same as managing standard target servers. See **Working with Target Servers** and the **CC-SG Administrators Guide** for more information. Any changes made to the blade chassis configuration in will be propagated to these client applications.

Important: When the CIM connecting the blade chassis to the Dominion device is powered down or disconnected from the Dominion device, all established connections to the blade chassis will be dropped. When the CIM is reconnected or powered up you will need to re-establish the connection(s).

Important: If you move a blade chassis from one Dominion device port to another Dominion device port, interfaces that were added to the blade chassis node in CC-SG will be lost in CC-SG. All other information will be retained.

Generic Blade Chassis Configuration

The Generic Blade Chassis' selection provides only a manual configuration mode of operation. See *Supported Blade Chassis Models* (on page 175), *Supported CIMs for Blade Chassis* (on page 176), and *Required and Recommended Blade Chassis Configurations* (on page 178) for important, additional information when configuring the blade chassis.

1. Connect the blade chassis to the KSX II. See Step 3: Connect the Equipment for details.

2. Select Device Settings > Port Configuration to open the Port Configuration page.

![Raritan.]

3. On the Port Configuration page, click on the name of the blade chassis you want to configure. The Port page will open.

4. Select the Blade Chassis radio button. The page will then display the necessary fields to configure a blade chassis.

5. Select Generic from the Blade Server Chassis Model drop-down.

6. Configure the blade chassis as applicable.

   a. Switch Hot Key Sequence - Define the hot key sequence that will be used to switch from KVM to the blade chassis. The Switch Hot Key Sequence must match the sequence used by the KVM module in the blade chassis.

   b. Administrative Module Primary IP Address/Host Name - Not applicable.

   c. Maximum Number of Slots - Enter the default maximum number of slots available on the blade chassis.

   d. Port Number - The default port number for the blade chassis is 22. Not applicable.

   e. Username - Not applicable.

   f. Password - Not applicable.

7. Change the blade chassis name if needed.

8. Indicate the blades that are installed in the blade chassis by checking the Installed checkbox next to each slot that has a blade installed. Alternatively, use the Select All checkbox. If needed, change the blade server names.

9. In the Blade Chassis Managed Links section of the page, you are able to configure the connection to a blade chassis web browser interface if one is available. Click the Blade Chassis Managed Links icon **► Blade Chassis Managed Links** to expand the section on the page.

   The first URL link is intended for use to connect to the blade chassis Administration Module GUI.

   Note: Access to the URL links entered in this section of the page is governed by the blade chassis port permissions.

   a. Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.

   b. URL - Enter the URL to the interface. Required

     c.   Username - Enter the username used to access the interface. Optional

     d.   Password - Enter the password used to access the interface. Optional

> *Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications or the connection will fail.*

     e.   The Username Field and Password Field, which are both optional, contain the labels that are expected to be associated with the username and password entries. It is in these fields you should enter the field names for the username and password fields used on the login screen for the web application. You can view the HTML source of the login screen to find the field *names*, not the field labels. See **Tips for Adding a Web Browser Interface** (on page 172) for tips on adding a web browser interface. **Optional**

10. USB profile information does not apply to a generic configuration.

11. In the Target Settings section, select 720x400 Compensation if you are experiencing display issues when the target is using this resolution.

12. Select 'Use international keyboard for scan code set 3' if connecting to the target with a DCIM-PS2 and require the use of scan code set 3 with an international keyboard.

13. Click OK to save the configuration.

Dell Blade Chassis Configuration

See **Supported Blade Chassis Models** (on page 175), **Supported CIMs for Blade Chassis** (on page 176), and **Required and Recommended Blade Chassis Configurations** (on page 178) for important, additional information when configuring the blade chassis. See **Dell Chassis Cable Lengths and Video Resolutions** (on page 307) for information on cable lengths and video resolutions when using Dell® chassis with the KSX II.

1. Connect the blade chassis to the KSX II. See Step 3: Connect the Equipment for details.

2. Select Device Settings > Port Configuration to open the Port Configuration page.

3. On the Port Configuration page, click on the name of the blade chassis you want to configure. The Port page will open.

4. Select the Blade Chassis radio button. The page will then display the necessary fields to configure a blade chassis.

5. Select the Dell blade chassis model from the Blade Server Chassis Model drop-down.

▶ **To configure a Dell PowerEdge M1000e:**

1. If you selected Dell PowerEdge™ M1000e, auto-discovery is available. Configure the blade chassis as applicable. Prior to configuring a blade chassis that can be auto-discovered, it must be configured to enable SSH connections on the designated port number (see Device Services). Additionally, a user account with the corresponding authentication credentials must be previously created on the blade chassis.

   a. Switch Hot Key Sequence - Select the hot key sequence that will be used to switch from KVM to the blade server. The Switch Hot Key Sequence must match the sequence used by the KVM module in the blade chassis.

   b. Maximum Number of Slots - The default maximum number of slots available on the blade chassis is automatically entered.

   c. Administrative Module Primary IP Address/Host Name - Enter the primary IP address for the blade chassis. **Required for auto-discovery mode**

   d. Port Number - The default port number for the blade chassis is 22. Change the port number if applicable. **Required for auto-discovery mode**

   e. Username - Enter the username used to access the blade chassis. **Required for auto-discovery mode**

   f. Password - Enter the password used to access the blade chassis. **Required for auto-discovery mode**

2. If you want the KSX II to auto-discover the chassis blades, select the Blade Auto-Discovery checkbox and then click the Discover Blades on Chassis Now button. Once the blades are discovered, they will be displayed on the page.

3. Change the blade chassis name if needed. If the chassis is already named, that information automatically populates this field. If it is not already named, the KSX II assigns the chassis a name. The default naming convention for the blade chassis by the KSX II is # Blade_Chassis_Port#.

4. If operating in Manual mode, indicate the blades that are installed in the blade chassis by checking the Installed checkbox next to each slot that has a blade installed. Alternatively, use the Select All checkbox. If needed, change the blade server names

   If operating in Auto-discovery mode, the Installed box will display the slots containing blades during discovery.

5. In the Blade Chassis Managed Links section of the page, you are able to configure the connection to a blade chassis web browser interface if one is available. Click the Blade Chassis Managed Links icon ▶ Blade Chassis Managed Links to expand the section on the page.

The first URL link is intended for use to connect to the blade chassis Administration Module GUI.

Note: Access to the URL links entered in this section of the page is governed by the blade chassis port permissions.

a.   Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required.   The username, password, username field and password field are optional depending on whether single sign-on is desired or not.

b.   URL - Enter the URL to the interface. See **Blade Chassis Sample URL Formats** (on page 180) for sample configurations for the Dell M1000e.

c.   Username - Enter the username used to access the interface.

d.   Password - Enter the password used to access the interface.

Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications or the connection will fail.

e.   The Username Field and Password Field, which are both optional, contain the labels that are expected to be associated with the username and password entries. It is in these fields you should enter the field names for the username and password fields used on the login screen for the web application. You can view the HTML source of the login screen to find the field *names*, not the field labels. See **Tips for Adding a Web Browser Interface** (on page 172) for tips on adding a web browser interface.

6.   USB profiles do not apply to Dell chassis.

7.   In the Target Settings section, select 720x400 Compensation if you are experiencing display issues when the target is using this resolution.

8.   Select 'Use international keyboard for scan code set 3' if connecting to the target with a DCIM-PS2 and require the use of scan code set 3 with an international keyboard.

9.   Click OK to save the configuration.

▶   **To configure a Dell PowerEdge 1855/1955:**

1.   If you selected Dell 1855/1955, auto-discovery *is not available*. Configure the blade chassis as applicable.

a.   Switch Hot Key Sequence - Select the hot key sequence that will be used to switch from KVM to the blade server.

b. Maximum Number of Slots - The default maximum number of slots available on the blade chassis is automatically entered.

c. Administrative Module Primary IP Address/Host Name - Not applicable.

d. Port Number - The default port number for the blade chassis is 22. Not applicable.

e. Username - Not applicable.

f. Password - Not applicable.

2. Change the blade chassis name if needed.

3. Indicate the blades that are installed in the blade chassis by checking the Installed checkbox next to each slot that has a blade installed. Alternatively, use the Select All checkbox. If needed, change the blade server names.

4. In the Blade Chassis Managed Links section of the page, you are able to configure the connection to a blade chassis web browser interface if one is available. Click the Blade Chassis Managed Links icon ▶ **Blade Chassis Managed Links** to expand the section on the page.

The first URL link is intended for use to connect to the blade chassis Administration Module GUI.

Note: Access to the URL links entered in this section of the page is governed by the blade chassis port permissions.

a. Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.

b. URL - Enter the URL to the interface. See ***Blade Chassis Sample URL Formats*** (on page 180) for sample configurations for the Dell PowerEdge 1855/1955.

c. Username - Enter the username used to access the interface.

d. Password - Enter the password used to access the interface.

Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications or the connection will fail.

e. The Username Field and Password Field, which are both optional, contain the labels that are expected to be associated with the username and password entries. It is in these fields you should enter the field names for the username and password fields used on the login screen for the web application. You can view the HTML source of the login screen to find the field *names*, not the field labels. See *Tips for Adding a Web Browser Interface* (on page 172) for tips on adding a web browser interface.

5. USB profiles do not apply to Dell chassis.

6. Click OK to save the configuration.

IBM Blade Chassis Configuration

See *Supported Blade Chassis Models* (on page 175), *Supported CIMs for Blade Chassis* (on page 176), and *Required and Recommended Blade Chassis Configurations* (on page 178) for important, additional information when configuring the blade chassis.

1. Connect the blade chassis to the KSX II. See Step 3: Connect the Equipment for details.

2. Select Device Settings > Port Configuration to open the Port Configuration page.

3. On the Port Configuration page, click on the name of the blade chassis you want to configure. The Port page will open.

4. Select the Blade Chassis radio button. The page will then display the necessary fields to configure a blade chassis.

5. Select the IBM® blade chassis model from the Blade Server Chassis Model drop-down.

▶ **To configure a IBM BladeCenter H and E:**

1. If you selected IBM BladeCenter® H or E, auto-discovery is available. Configure the blade chassis as applicable. Prior to configuring a blade chassis that can be auto-discovered, it must be configured to enable SSH connections on the designated port number (see Device Services). Additionally, a user account with the corresponding authentication credentials must be previously created on the blade chassis. The KSX II only supports auto-discovery for AMM[1].

   a. Switch Hot Key Sequence - Predefined.

   b. Maximum Number of Slots - The default maximum number of slots available on the blade chassis is automatically entered.

   c. Administrative Module Primary IP Address/Host Name - Enter the primary IP address for the blade chassis. **Required for auto-discovery mode**

    d. Port Number - The default port number for the blade chassis is 22. Change the port number if applicable. **Required for auto-discovery mode**

    e. Username - Enter the username used to access the blade chassis. **Required for auto-discovery mode**

    f. Password - Enter the password used to access the blade chassis. **Required for auto-discovery mode**

2. If you want the KSX II to auto-discover the chassis blades, select the Blade Auto-Discovery checkbox and then click the Discover Blades on Chassis Now button. Once the blades are discovered, they will be displayed on the page.

3. Change the blade chassis name if needed. If the chassis is already named, that information automatically populates this field. If it is not already named, the KSX II assigns the chassis a name. The default naming convention for the blade chassis by the KSX II is # Blade_Chassis_Port#.

4. If operating in Manual mode, indicate the blades that are installed in the blade chassis by checking the Installed checkbox next to each slot that has a blade installed. Alternatively, use the Select All checkbox. If needed, change the blade server names

   If operating in Auto-discovery mode, the Installed box will display the slots containing blades during discovery.

5. In the Blade Chassis Managed Links section of the page, you are able to configure the connection to a blade chassis web browser interface if one is available. Click the Blade Chassis Managed Links icon to expand the section on the page.

   The first URL link is intended for use to connect to the blade chassis Administration Module GUI.

   Note: Access to the URL links entered in this section of the page is governed by the blade chassis port permissions.

    a. Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.

    b. URL - Enter the URL to the interface. See ***Blade Chassis Sample URL Formats*** (on page 180) for sample configurations for the IBM BladeCenter.

    c. Username - Enter the username used to access the interface.

    d. Password - Enter the password used to access the interface.

Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications or the connection will fail.

    e. The Username Field and Password Field, which are both optional, contain the labels that are expected to be associated with the username and password entries. It is in these fields you should enter the field names for the username and password fields used on the login screen for the web application. You can view the HTML source of the login screen to find the field *names*, not the field labels. See ***Tips for Adding a Web Browser Interface*** (on page 172) for tips on adding a web browser interface.

6. If applicable, define the USB profile for the blade chassis or select an existing USB profile. Click the USB Profiles Select USB Profiles for

    Port icon   **► Select USB Profiles for Port**   or the Apply Select Profiles

    to Other Ports icon   **► Apply Selected Profiles to Other Ports**   to expand these sections of the page. See ***Configuring USB Profiles (Port Page)*** (on page 181).

7. Click OK to save the configuration.

►   **To configure a IBM BladeCenter (Other):**

1. If you selected IBM BladeCenter (Other), auto-discovery *is not* available. Configure the blade chassis as applicable.

    a. Switch Hot Key Sequence - Select the hot key sequence that will be used to switch from KVM to the blade server.

    b. Administrative Module Primary IP Address/Host Name - Enter the primary IP address for the blade chassis. Not applicable.

    c. Maximum Number of Slots - Enter the default maximum number of slots available on the blade chassis.

    d. Port Number - The default port number for the blade chassis is 22. Not applicable.

    e. Username - Not applicable.

    f. Password - Not applicable.

2. Change the blade chassis name if needed.

3. Indicate the blades that are installed in the blade chassis by checking the Installed checkbox next to each slot that has a blade installed.   Alternatively, use the Select All checkbox.   If needed, change the blade server names. If it is not already named, the KSX II assigns a name to the blade server. The default blade server naming convention is # Blade_Chassis_Port#_Slot#.

4. In the Blade Chassis Managed Links section of the page, you are able to configure the connection to a blade chassis web browser interface if one is available. Click the Blade Chassis Managed Links icon ► **Blade Chassis Managed Links** to expand the section on the page.

The first URL link is intended for use to connect to the blade chassis Administration Module GUI.

Note: Access to the URL links entered in this section of the page is governed by the blade chassis port permissions.

a. Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.

b. URL - Enter the URL to the interface. See **Blade Chassis Sample URL Formats** (on page 180) for sample configurations for the IBM BladeCenter.

c. Username - Enter the username used to access the interface.

d. Password - Enter the password used to access the interface.

Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications or the connection will fail.

e. The Username Field and Password Field, which are both optional, contain the labels that are expected to be associated with the username and password entries. It is in these fields you should enter the field names for the username and password fields used on the login screen for the web application. You can view the HTML source of the login screen to find the field *names*, not the field labels. See **Tips for Adding a Web Browser Interface** (on page 172) for tips on adding a web browser interface.

5. USB profiles are not used by IBM (Other) configurations.

6. In the Target Settings section, select 720x400 Compensation if you are experiencing display issues when the target is using this resolution.

7. Select 'Use international keyboard for scan code set 3' if connecting to the target with a DCIM-PS2 and require the use of scan code set 3 with an international keyboard.

8. Click OK to save the configuration.

Tips for Adding a Web Browser Interface

You can add a Web Browser Interface to create a connection to a device with an embedded web server.   A Web Browser interface can also be used to connect to any web application, such as the web application associated with an RSA, DRAC or ILO Processor card.

You must have DNS configured or URLs will not resolve. You do not need to have DNS configured for IP addresses.

▶ **To add a web browser interface:**

1. The default name for a Web Browser Interface is provided. If needed, change the name in the Name field.

2. Enter the URL or domain name for the web application in the URL field. You must enter the URL at which the web application expects to read the username and password.

   Follow these examples for correct formats:

   ▪ http(s)://192.168.1.1/login.asp

   ▪ http(s)://www.example.com/cgi/login

   ▪ http(s)://example.com/home.html

3. Enter the username and password that will allow access to this interface. **Optional**

4. If username and password were entered, in the Username Field and Password Field, type the field names for the username and password fields that are used in the login screen for the web application. You must view the HTML source of the login screen to find the field names, not the field labels.

Tip for locating field names:

- In the HTML source code for the login page of the web application, search for the field's label, such as Username and Password.

- When you find the field label, look in the adjacent code for a tag that looks like this: name="user". The word in quotes is the field name.

HP Blade Chassis Configuration (Port Group Management)

The KSX II supports the aggregation of ports connected to certain types of blades into a group representing the blade chassis. Specifically, HP® BladeServer blades and Dell® PowerEdge™ 1855/1955 blades when the Dell PowerEdge 1855/1955 is connected from each individual blade to a port on the KSX II.

The chassis is identified by a Port Group Name and the group is designated as a Blade Server Group on the Port Group Management page. Port Groups consist solely of ports configured as standard KVM ports, not ports configured as blade chassis. A port may only be a member of a single group.

Ports connected to integrated KVM modules in a blade chassis are configured as blade chassis subtypes. These ports are eligible to be included in port groups.

When KSX II ports are connected to integrated KVM modules in a blade chassis and not to individual blades, the ports are configured as blade chassis subtypes.   These ports are not eligible to be included in port groups and will not appear in the Select Port for Group, Available list.

If a standard KVM port has been included in a port group, and then is subsequently repurposed for use as a blade chassis subtype, it must first be removed from the port group.

Port Groups are restored using the Backup and Restore option (see **Backup and Restore** (on page 207)).
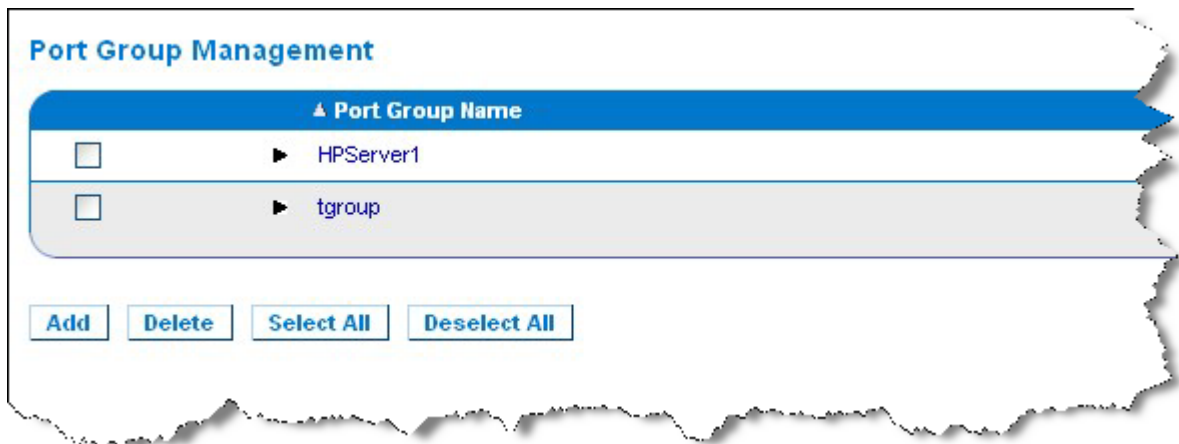
▶   **To add a port group:**

1. Click Device Settings > Port Group Management to open the Port Group Management page.

2. Click the Add button to open the Port Group page.

3. Enter a Port Group Name. The port group name is not case sensitive and can contain up to 32 characters.

4. Select the Blade Server Group checkbox.

   If you want to designate that these ports are attached to blades housed in a blade chassis (for example, HP c3000 or Dell PowerEdge 1855), select the Blade Server Group checkbox.

   Note: This is especially important to CC-SG users who want HP blades to be organized on a chassis basis, although each blade has its own connection to a port on the KSX II.

5. Click on a port in the Available box in the Select Ports for Group section. Click Add to add the port to the group. The port will be moved to the Selected box.

6. Click OK to add the port group.

Port Group

Port Group Name
HPServer1   ☑ **Blade Server Group**

Select Ports for Group

Available: **Selected:**

                                                                 Dominion_KX2_Port8

                          Add >

                        < Remove

OK   Cancel

▶ **To edit port group information:**

1. On the Port Group Management page, click on the link of the port group you want to edit. The Port Group page opens.

2. Edit the information as needed.

3. Click OK to save the changes.

▶ **To delete a port group:**

1. Click on the Port Group Management page, select the checkbox of the port group you want to delete.

2. Click the Delete button.

3. Click OK on the warning message.

Supported Blade Chassis Models

This table contains the blade chassis models that are supported by the KSX II and the corresponding profiles that should be selected per chassis model when configuring them in the KSX II application. A list of these models can be selected on the Port Configuration page from the Blade Server Chassis Model drop-down, which appears when the Blade Chassis radio button is selected. For details on how to configure each blade chassis model, see their corresponding topics in this section of the help.

Blade chassis model	KSX II Profile
Dell® PowerEdge™ 1855/1955	Dell PowerEdge 1855/1955
Dell PowerEdge M1000e	Dell PowerEdge M1000e
IBM® BladeCenter® S	IBM (Other)
IBM BladeCenter H	IBM BladeCenter H
IBM BladeCenter T	IBM (Other)
IBM BladeCenter HT	IBM (Other)
IBM BladeCenter E	IBM BladeCenter E
HP®	Configure using Port Group Management functions. See *HP Blade Chassis Configuration (Port Group Management)* (on page 173).

Supported CIMs for Blade Chassis

The following CIMs are supported for blade chassis being managed through the KSX II:

- DCIM-PS2
- DCIM-USBG2
- D2CIM-VUSB
- D2CIM-DVUSB

Following is a table containing supported CIMs for each blade chassis model that the KSX II supports.

Blade chassis	Connection method	Recommended CIM(s)
Generic	If a D2CIM-VUSB or D2CIM-DVUSB is used when connecting to a blade-chassis configured as Generic, you will be able to select the USB profiles from the Port Configuration page and the client's USB Profile menu. However, virtual media is not supported for generic blade chassis and the Virtual Media menu is disabled on the client.	• DCIM-PS2 • DCIM-USBG2
Dell® PowerEdge™ 1855	Includes one of the three KVM modules : • Analog KVM Ethernet switch module (standard) • Digital Access KVM switch module (optional) • KVM switch module (standard on systems sold prior to April, 2005) These switches provide a custom connector that allows two PS/2 and one video device to be connected to the system. Source: *Dell PowerEdge 1855 User Guide*	• DCIM-PS2
Dell PowerEdge 1955	One of two types of KVM modules may be installed: • Analog KVM switch module • Digital Access KVM switch module Both modules enable you to connect a PS/2-compatible keyboard, mouse and video monitor to the system (using a custom cable provided with the system). Source: *Dell PowerEdge 1955 Owner's Manual*	• DCIM-PS2
Dell PowerEdge	The KVM Switch Module (iKVM) is Integrated	• DCIM-USBG2

Blade chassis	Connection method	Recommended CIM(s)
M1000e	with this chassis. The iKVM is compatible with the following peripherals: • USB keyboards, USB pointing devices • VGA monitors with DDC support. Source: *Dell Chassis Management Controller, Firmware Version 1.0, User Guide*	
HP® BladeSystem c3000	The HP c-Class Blade SUV Cable enables you to perform blade chassis administration, configuration, and diagnostic procedures by connecting video and USB devices directly to the server blade. Source: *HP Proliant™ BL480c Server Blade Maintenance and Service Guide*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (for standard KVM port operation without a KVM option)
HP BladeSystem c7000	The HP c-Class Blade SUV Cable enables you to perform server blade administration, configuration, and diagnostic procedures by connecting video and USB devices directly to the server blade. Source: *HP ProLiant BL480c Server Blade Maintenance and Service Guide*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (for standard KVM port operation)
IBM® BladeCenter® S	The Advanced Management Module (AMM) provides system management functions and keyboard/video/mouse (KVM) multiplexing for all blade chassis. The AMM connections include: a serial port, video connection, remote management port (Ethernet), and two USB v2.0 ports for a keyboard and mouse. Source: *Implementing the IBM BladeCenter S Chassis*	• DCIM-USBG2
IBM BladeCenter H	The BladeCenter H chassis ships standard with one Advanced Management Module. Source: *IBM BladeCenter Products and Technology*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter E	The current model BladeCenter E chassis (8677-3Rx) ships standard with one Advanced Management Module. Source: *IBM BladeCenter Products and Technology*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter T	The BladeCenter T chassis ships standard with	• DCIM-PS2

Blade chassis	Connection method	Recommended CIM(s)
	one Advanced Management Module.	
	In contrast to the standard BladeCenter chassis, the KVM module and the Management Module in the BladeCenter T chassis are separate components. The front of the Management Module only features the LEDs for displaying status. All Ethernet and KVM connections are fed through to the rear to the LAN and KVM modules.	
	The KVM module is a hot swap module at the rear of the chassis providing two PS/2 connectors for keyboard and mouse, a systems-status panel, and a HD-15 video connector.	
	Source: *IBM BladeCenter Products and Technology*	
IBM BladeCenter HT	The BladeCenter HT chassis ships standard with one Advanced Management Module. This module provides the ability to manage the chassis as well as providing the local KVM function.	• DCIM-USBG2
	Source: *IBM BladeCenter Products and Technology*	

Note: In order to support Auto-discovery, IBM BladeCenter Models H and E must use AMM with firmware version BPET36K or later.

Note: In the case of IBM Blade Center Models E and H, the KSX II only supports auto-discovery for AMM[1] as the acting primary management module.

Required and Recommended Blade Chassis Configurations

This table contains information on limitations and constraints that apply to configuring blade chassis to work with the KSX II. Raritan recommends that all of the information below is followed.

Blade chassis	Required/recommended action
Dell® PowerEdge™ M1000e	• Disable the iKVM GUI screensaver. An authorize dialog will appear, preventing iKVM from working correctly, if this is not done. • Exit the iKVM GUI menu before attaching Dell's chassis to a Raritan CIM. iKVM may not work correctly if this is not done. • Configure the iKVM GUI Main menu to select target blades by

Blade chassis	Required/recommended action
	Slot, not by Name. iKVM may not work correctly if this is not done.
	• *Do not* designate any slots for scan operations in the iKVM GUI Setup Scan menu. iKVM may not work correctly otherwise.
	• *Do not* designate any slots for broadcast keyboard/mouse operations in the iKVM GUI Setup Broadcast menu. iKVM may not work correctly otherwise.
	• Designate a single key sequence to invoke the iKVM GUI. This key sequence must also be identified during KSX II port configuration. Otherwise, indiscriminate iKVM operation may occur as a result of client key entry.
	• Ensure that Front Panel USB/Video Enabled is *not* selected during iKVM configuration via the Dell CMC GUI. Otherwise, connections made at the front of chassis will take precedence over the KSX II connection at the rear, preventing proper iKVM operation. A message will be displayed stating 'User has been disabled as front panel is currently active.'
	• Ensure that 'Allow access to CMC CLI from iKVM' is *not* selected during iKVM configuration via the Dell CMC GUI.
	• To avoid having the iKVM GUI display upon connecting to the blade chassis, set the Screen Delay Time to 8 seconds.
	• Recommend that 'Timed' and 'Displayed' be selected during iKVM GUI Flag Setup. This will allow you to visually confirm the connection to the desired blade slot.
Dell PowerEdge 1855/1955	• Disable the iKVM GUI screensaver. An Authorize dialog will appear if this is not done and will prevent the iKVM from operating correctly.
	• Exit the iKVM GUI menu before attaching Dell's chassis to a Raritan CIM. iKVM may not work correctly if this is not done.
	• Configure the iKVM GUI Main menu to select target blades by Slot, not by Name. iKVM may not work correctly if this is not done.
	• *Do not* designate any slots for scan operations in the iKVM GUI Setup Scan menu or the iKVM may not work properly.
	• To avoid having the iKVM GUI display upon connecting to the blade chassis, set the Screen Delay Time to 8 seconds.
	• Recommend that 'Timed' and 'Displayed' be selected during iKVM GUI Flag Setup. This will allow you to visually confirm the connection to the desired blade slot.
IBM®/Dell® Auto-Discovery	• It is recommended that Auto-Discovery be enabled when applying blade level access permissions. Otherwise, set access permissions on a blade-chassis wide basis.
	• Secure Shell (SSH) must be enabled on the blade chassis

Blade chassis	Required/recommended action
	management module.
	• The SSH port configured on the blade chassis management module and the port number entered on the Port Configuration page must match.
IBM KX2 Virtual Media	• Raritan KSX II virtual media is supported only on IBM BladeCenter® Models H and E. This requires the use of the D2CIM-DVUSB. The black D2CIM-DVUSB Low-Speed USB connector is attached to the Administrative Management Module (AMM) at the rear of the unit. The gray D2CIM-DVUSB High-Speed USB connector is attached to the Media Tray (MT) at the front of the unit. This will require a USB extension cable.

Note: All IBM BladeCenters that use AMM must use AMM firmware version BPET36K or later to work with the KSX II.

Note: In the case of IBM Blade Center Models E and H, the KSX II only supports auto-discovery for AMM[1] as the acting primary management module.

Blade Chassis Sample URL Formats

This table contains sample URL formats for blade chassis being configured in the KSX II.

Blade chassis	Sample URL format
Dell® M1000e	• URL: https://192.168.60.44/cgi-bin/webcgi/login
	• Username: root
	• Username Field: user
	• Password: calvin
	• Password Field: password
Dell 1855	• URL: https://192.168.60.33/Forms/f_login
	• Username: root
	• Username Field: TEXT_USER_NAME
	• Password: calvin
	• Password Field: TEXT_PASSWORD
IBM® BladeCenter® E or H	• http://192.168.84.217/private/welcome.ssi

Configuring USB Profiles (Port Page)

You choose the available USB profiles for a port in the Select USB Profiles for Port section of the Port page. The USB profiles chosen in the Port page become the profiles available to the user in VKC when connecting to a KVM target server from the port. The default is the Windows 2000® operating system, Windows XP® operating system, Windows Vista® operating system profile. For information about USB profiles, see ***USB Profiles*** (on page 104).

Note: To set USB profiles for a port, you must have a VM-CIM or Dual VM-CIM connected with firmware compatible with the current firmware version of the KSX II. See Upgrading CIMs.

The profiles available to assign to a port appear in the Available list on the left. The profiles selected for use with a port appear in the Selected list on the right. When you select a profile in either list, a description of the profile and its use appears in the Profile Description field.

In addition to selecting a set of profiles to make available for a KVM port, you can also specify the preferred profile for the port and apply the settings set for one port other KVM ports.

Note: See **Mouse Modes when Using the Mac OS-X USB Profile with a DCIM-VUSB** *(on page 112) for information on using the Mac OS-X® USB profile if you are using a DCIM-VUSB or DCIM-DVUSB.*

► **To open the Port page:**

1. Choose Device Settings > Port Configuration. The Port Configuration page opens.

2. Click the Port Name for the KVM port you want to edit. The Port page opens.

► **To select the USB profiles for a KVM port:**

1. In the Select USB Profiles for Port section, select one or more USB profiles from the Available list.

   ▪ Shift-Click and drag to select several continuous profiles.

- Ctrl-Click to select several discontinuous profiles.
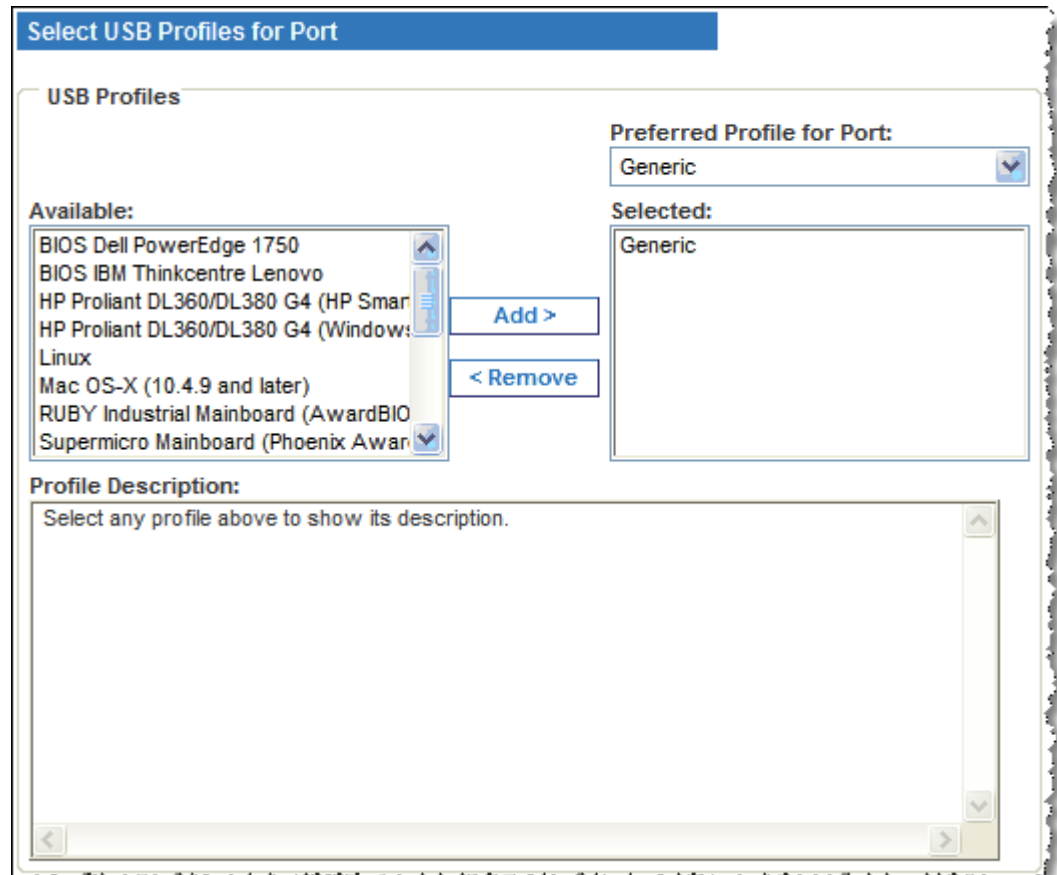
2. Click Add. The selected profiles appear in the Selected list. These are the profiles that can be used for the KVM target server connected to the port.

▶ **To specify a preferred USB profile:**

1. After selecting the available profiles for a port, choose one from the Preferred Profile for Port menu. The default is Generic. The selected profile will be used when connecting to the KVM target server. You can change to any other USB profile as necessary.

▶ **To remove selected USB profiles:**

1. In the Select USB Profiles for Port section, select one or more profiles from the Selected list.

   - Shift-Click and drag to select several continuous profiles.

   - Ctrl-Click to select several discontinuous profiles.

2. Click Remove. The selected profiles appear in the Available list. These profiles are no longer available for a KVM target server connected to this port.

▶ **To apply a profile selection to multiple ports:**

1. In the Apply Selected Profiles to Other Ports section, select the Apply checkbox for each KVM port you want to apply the current set of selected USB profiles to.

▼ Apply Selected Profiles to Other Ports			
Apply	Port Number	Port Name	Selected USB Profiles
☐	3	vm-cim #1	Generic, Troubleshooting 1, Troubleshooting 2, Troubleshooting 3
	5	vm-cim #2	CIM firmware upgrade required!
☑	15	charles_cim - vm-cim #3	Generic, Troubleshooting 1, Troubleshooting 2, Troubleshooting 3

| OK | Select All | Deselect All | Cancel |

- To select all KVM ports, click Select All.
- To deselect all KVM ports, click Deselect All.

Configuring KSX II Local Port Settings

From the Local Port Settings page, you can customize many settings for the KSX II Local Console including keyboard, hot keys, video switching delay, power save mode, local user interface resolution settings, and local user authentication. Further, you can change a USB profile from the local port.

▶ **To configure the local port settings:**

Note: Some changes you make to the settings on the Local Port Settings page will restart the browser you are working in. If a browser restart will occur when a setting is changed, it is noted in the steps provider here.

1. Choose Device Settings > Local Port Settings. The Local Port Settings page opens.

2. Select the checkbox next to the Enable Standard Local Port to enable it. Deselect the checkbox to disable it. By default, the standard local port is enabled but can be disabled as needed. The browser will be restarted when this change is made.

3. Choose the appropriate keyboard type from among the options in the drop-down list. The browser will be restarted when this change is made.

   - US

   - US/International

   - United Kingdom

   - French (France)

- German (Germany)
- JIS (Japanese Industry Standard)
- Simplified Chinese
- Traditional Chinese
- Dubeolsik Hangul (Korean)
- German (Switzerland)
- Portuguese (Portugal)
- Norwegian (Norway)
- Swedish (Sweden)
- Danish (Denmark)
- Belgian (Belgium)

Note: Keyboard use for Chinese, Japanese, and Korean is for display only. Local language input is not supported at this time for KSX II Local Console functions.

4. Choose the local port hotkey. The local port hotkey is used to return to the KSX II Local Console interface when a target server interface is being viewed. The default is to Double Click Scroll Lock, but you can select any key combination from the drop-down list:

Hot key:	Take this action:
Double Click Scroll Lock	Press Scroll Lock key twice quickly
Double Click Num Lock	Press Num Lock key twice quickly
Double Click Caps Lock	Press Caps Lock key twice quickly
Double Click Left Alt key	Press the left Alt key twice quickly
Double Click Left Shift key	Press the left Shift key twice quickly
Double Click Left Ctrl key	Press the left Ctrl key twice quickly

5. Select the Local Port Connect key. Use a connect key sequence to connect to a target and switch to another target. You can then use the hot key to disconnect from the target and return to the local port GUI. The connect key works for both standard servers and blade chassis. Once the local port connect key is created, it will appear in the Navigation panel of the GUI so you can use it as a reference. See **Connect Key Examples** (on page 247) for examples of connect key sequences.

6. Set the Video Switching Delay from between 0 - 5 seconds, if necessary. Generally 0 is used unless more time is needed (certain monitors require more time to switch the video).

7. If you would like to use the power save feature.

    a.   Select the Power Save Mode checkbox.

    b.   Set the amount of time (in minutes) in which Power Save Mode will be initiated.

8. Choose the resolution for the KSX II Local Console from the drop-down list. The browser will be restarted when this change is made.

- 800x600

- 1024x768

- 1280x1024

9. Choose the refresh rate from the drop-down list. The browser will be restarted when this change is made.

- 60 Hz

- 75 Hz

10. Choose the type of local user authentication.

- Local/LDAP/RADIUS. This is the recommended option. For more information about authentication, see *Remote Authentication* (on page 36).

- None. There is no authentication for Local Console access. This option is recommended for secure environments only.

- Select the "Ignore CC managed mode on local port" checkbox if you would like local user access to the KSX II even when the device is under CC-SG management.

Note: If you initially choose not to ignore CC Manage mode on the local port but later want local port access, you will have to remove the device from under CC-SG management (from within CC-SG). You will then be able to check this checkbox.

11. Click OK.

Port Keywords

Port keywords work as a filter. If a keyword is detected, a corresponding message be logged in a local port log and a corresponding trap will be sent via SNMP (if configured).

Defining keywords guarantees that only messages that contain those keywords are logged for the local port.

You can create port keywords and associate them with:

- Syslog
- Audit log
- SNMP traps

▶ **To define keywords and associate them with a port:**

1. Choose Device Settings > Port Keyword List > Keyword. The Port Keyword List page will open.

Home > Device Settings > Port Keyword List

Port Keyword List

	▲ Keyword	Port Number	Port Name
☐	panic	9	Cisco 2501
☐	Partial	9	Cisco 2501
☐	question	9	Cisco 2501

Add   Delete

If no keywords have been created yet, the page will contain the message *"There are no port keywords defined"*. If port keywords do exist, they will be listed on the Port Keyword List page.

2. Define a keyword for the first time, by clicking the Add button on the Port Keyword List page. The Add Keyword page will then open. Follow steps 3 - 5 to create new keywords.

3. Type a keyword in the Keyword field and then click the Add button. The keyword will be added to the page directly under the Keyword field and will appear on the Port Keyword List page once OK is selected. Add additional keywords by following the same steps (if needed).

4. In the Ports section of the page in the Available selection box, click the port or ports you want to associate with that keyword and click Add. The port associated with the keyword will then be moved to the Selected selection box. Continue adding ports as needed.

5. Click OK.

▶ **To remove ports from the selected list:**

1. On the Add Keyword page, click the port in the Selected selection box and then click Remove.

▶ **To delete keywords:**

1. On the Port Keyword List page, check the checkbox of the keyword you would like to delete.

2. Click the Delete button. A warning message will be displayed.

3. Click OK in the warning message.

Port Group Management

This function is specific to HP blade chassis configuration. See *HP Blade Chassis Configuration (Port Group Management)* (on page 173).

Chapter 9   Security Management

In This Chapter

Security Settings

From the Security Settings page, you can specify login limitations, user blocking, password rules, and encryption and share settings.

Raritan SSL certificates are used for public and private key exchanges, and provide an additional level of security. Raritan web server certificates are self-signed. Java applet certificates are signed by a VeriSign certificate. Encryption guarantees that your information is safe from eavesdropping and these certificates ensure that you can trust that the entity is Raritan, Inc.

▶   **To configure the security settings:**

1. Choose Security > Security Settings. The Security Settings page opens.

2. Update the *Login Limitations* (on page 190) settings as appropriate.

3. Update the *Strong Passwords* (on page 191) settings as appropriate.

4. Update the *User Blocking* (on page 192) settings as appropriate.

5. Update the Encryption & Share settings as appropriate.

6. Click OK.

▶ **To reset back to defaults:**

• Click Reset to Defaults.

Login Limitations		User Blocking	
☐ Enable Single Login Limitation		⦿ Disabled	
☐ Enable Password Aging		○ Timer Lockout	
Password Aging Interval (days)		Attempts	
60		3	
☐ Log Out Idle Users		Lockout Time	
Idle Timeout (minutes)		5	
30		○ Deactivate User-ID	
		Failed Attempts	
		3	

Strong Passwords	Encryption & Share
☐ Enable Strong Passwords	Encryption Mode
	Auto ▾
Minimum length of strong password	☑ Apply Encryption Mode to KVM and Virtual Media (Forced in FIPS 140-2 Mode)
8	☐ Enable FIPS 140-2 Mode (Changes are activated on reboot only!)
Maximum length of strong password	Current FIPS status: Inactive
16	PC Share Mode
☑ Enforce at least one lower case character	Private ▾
☑ Enforce at least one upper case character	☐ VM Share Mode
☑ Enforce at least one numeric character	Local Device Reset Mode
☑ Enforce at least one printable special character	Enable Local Factory Reset ▾
Number of restricted passwords based on history	
5	

OK   Reset To Defaults   Cancel

Login Limitations

Using login limitations, you can specify restrictions for single login, password aging, and the logging out idle users.

Limitation	Description
Enable single login limitation	When selected, only one login per user name is allowed at any time. When deselected, a given user name/password combination can be connected into the device from several client workstations simultaneously.
Enable password aging	When selected, all users are required to change their passwords periodically based on the number of days specified in Password Aging Interval field. This field is enabled and required when the Enable Password Aging checkbox is selected. Enter the number of days after which a password

Limitation	Description
	change is required. The default is 60 days.
Log out idle users, After (1-365 minutes)	Select the "Log off idle users" checkbox to automatically disconnect users after the amount of time you specify in the "After (1-365 minutes)" field. If there is no activity from the keyboard or mouse, all sessions and all resources are logged out. If a virtual media session is in progress, however, the session does not timeout.
	The After field is used to set the amount of time (in minutes) after which an idle user will be logged out. This field is enabled when the Log Out Idle Users option is selected. Up to 365 minutes can be entered as the field value

Strong Passwords

Strong passwords provide more secure local authentication for the system. Using strong passwords, you can specify the format of valid KSX II local passwords such as minimum and maximum length, required characters, and password history retention.

Strong passwords require user-created passwords to have a minimum of 8 characters with at least one alphabetical character and one nonalphabetical character (punctuation character or number). In addition, the first four characters of the password and the user name cannot match.

When selected, strong password rules are enforced. Users with passwords not meeting strong password criteria will automatically be required to change their password on their next login. When deselected, only the standard format validation is enforced. When selected, the following fields are enabled and required:

Field	Description
Minimum length of strong password	Passwords must be at least 8 characters long. The default is 8, but it can be up to 63.
Maximum length of strong password	The default is 16, but can be up to 64 characters long.
Enforce at least one lower case character	When checked, at least one lower case character is required in the password.
Enforce at least one upper case character	When checked, at least one upper case character is required in the password.
Enforce at least one	When checked, at least one numeric

Field	Description
numeric character	character is required in the password.
Enforce at least one printable special character	When checked, at least one special character (printable) is required in the password.
Number of restricted passwords based on history	This field represents the password history depth. That is, the number of prior passwords that cannot be repeated. The range is 1-12 and the default is 5.

User Blocking

The User Blocking options specify the criteria by which users are blocked from accessing the system after the specified number of unsuccessful login attempts.

The three options are mutually exclusive:

Option	Description
Disabled	The default option. Users are not blocked regardless of the number of times they fail authentication.

Option	Description
Timer Lockout	Users are denied access to the system for the specified amount of time after exceeding the specified number of unsuccessful login attempts. When selected, the following fields are enabled: ▪ Attempts - The number of unsuccessful login attempts after which the user will be locked out. The valid range is 1 - 10 and the default is 3 attempts. ▪ Lockout Time - The amount of time for which the user will be locked out. The valid range is 1 - 1440 minutes and the default is 5 minutes. *Note: Users in the role of Administrator are exempt from the timer lockout settings.*
Deactivate User-ID	When selected, this option specifies that the user will be locked out of the system after the number of failed login attempts specified in the Failed Attempts field: ▪ Failed Attempts - The number of unsuccessful login attempts after which the user's User-ID will be deactivated. This field is enabled when the Deactivate User-ID option is selected. The valid range is 1 - 10.

When a user-ID is deactivated after the specified number of failed attempts, the administrator must change the user password and activate the user account by selecting the Active checkbox on the User page.

Encryption & Share

Using the Encryption & Share settings you can specify the type of encryption used, PC and VM share modes, and the type of reset performed when the KSX II Reset button is pressed.

WARNING: If you select an encryption mode that is not supported by your browser, you will not be able to access the KSX II from your browser.

1. Choose one of the options from the Encryption Mode drop-down list. When an encryption mode is selected, a warning appears, stating that if your browser does not support the selected mode, you will not be able to connect to the KSX II. The warning states "When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the KSX II."

Encryption mode	Description
Auto	This is the recommended option. The KSX II autonegotiates to the highest level of encryption possible. You *must* select Auto in order for the device and client to successfully negotiate the use of FIPS compliant algorithms.
RC4	Secures user names, passwords and KVM data, including video transmissions using the RSA RC4 encryption method. This is a 128-bit Secure Sockets Layer (SSL) protocol that provides a private communications channel between the KSX II device and the Remote PC during initial connection authentication. If you enable FIPS 140-2 mode and RC4 has been selected, you will receive an error message. RC4 is not available while in FIPS 140-2 mode.
AES-128	The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data. 128 is the key length. When AES-128 is specified, be certain that your browser supports it, otherwise you will not be able to connect. See ***Checking Your Browser for AES Encryption*** (on page 196) for more information.
AES-256	The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data. 256 is the key length. When AES-256 is specified, be certain that your browser supports it, otherwise you will not be able to connect. See ***Checking Your Browser for AES Encryption*** (on page 196) for more information.

Note: MPC will always negotiate to the highest encryption and will match the Encryption Mode setting if not set to Auto.

Note: If you are running Windows XP® operating system with Service Pack 2, Internet Explorer® 7 cannot connect remotely to the KSX II using AES-128 encryption.

E≋E Raritan.

2. Apply Encryption Mode to KVM and Virtual Media. When selected, this option applies the selected encryption mode to both KVM and virtual media. After authentication, KVM and virtual media data is also transferred with 128-bit encryption.

3. For government and other high security environments, enable FIPS 140-2 Mode by selecting the Enable FIPS 140-2 checkbox. See **Enabling FIPS 140-2** (on page 196) for information on enabling FIPS 140-2.

4. PC Share Mode. Determines global concurrent remote KVM access, enabling up to eight remote users to simultaneously log into one KSX II and concurrently view and control the same target server through the device. Click the drop-down list to select one of the following options:

   ▪ Private - No PC share. This is the default mode. Each target server can be accessed exclusively by only one user at a time.

   ▪ PC-Share - KVM target servers can be accessed by up to eight users (administrator or non-administrator) at one time. Each remote user has equal keyboard and mouse control, however, note that uneven control will occur if one user does not stop typing or moving the mouse.

5. If needed, select VM Share Mode. This option is enabled only when PC-Share mode is enabled. When selected, this option permits the sharing of virtual media among multiple users, that is, several users can access the same virtual media session. The default is disabled.

6. If needed, select Local Device Reset Mode. This option specifies which actions are taken when the hardware Reset button (at the back of the device) is depressed. For more information, see Resetting the KSX II Using the Reset Button. Choose one of the following options:

Local device reset mode	Description
Enable Local Factory Reset (default)	Returns the KSX II device to the factory defaults.
Enable Local Admin Password Reset	Resets the local administrator password only. The password is reset to raritan.
Disable All Local Resets	No reset action is taken.

Note: When using the P2CIM-AUSBDUAL or P2CIM-APS2DUAL to attach a target to two KSX IIs, if Private access to the targets is required, both KVM switches must have Private set as their PC Share Mode.

See **Supported Paragon CIMS and Configurations** (on page 275) for additional information on using Paragon CIMs with the KSX II.

Checking Your Browser for AES Encryption

The KSX II supports AES-256. If you do not know if your browser uses AES, check with the browser manufacturer or navigate to the https://www.fortify.net/sslcheck.html website using the browser with the encryption method you want to check. This website detects your browser's encryption method and displays a report.

Note: Internet Explorer® 6 does not support AES 128 or 256-bit encryption.

AES 256 Prerequisites and Supported Configurations

AES 256-bit encryption is supported on the following web browsers only:

- Firefox® 2.0.0.x and 3.0.x and higher
- Internet Explorer 7 and 8

In addition to browser support, AES 256-bit encryption requires the installation of Java™ Cryptography Extension® (JCE®) Unlimited Strength Jurisdiction Policy Files.

Jurisdiction files for various JREs™ are available at the "other downloads" section of the following link:

- JRE1.6 - http://java.sun.com/javase/downloads/index_jdk5.jsp

Enabling FIPS 140-2

For government and other high security environments, enabling FIPS 140-2 mode may be desirable. The KSX II uses an embedded FIPS 140-2-validated cryptographic module running on a Linux® platform per FIPS 140-2 Implementation Guidance section G.5 guidelines. Once this mode is enabled, the private key used to generate the SSL certificates must be internally generated; it cannot be downloaded or exported.

▶ **To enable FIPS 140-2:**

1. Access the Security Settings page.

2. Enable FIPS 140-2 Mode by selecting the Enable FIPS 140-2 checkbox in the Encryption & Share section of the Security Settings page. You will utilize FIPS 140-2 approved algorithms for external communications once in FIPS 140-2 mode. The FIPS cryptographic module is used for encryption of KVM session traffic consisting of video, keyboard, mouse, virtual media and smart card data.

3. Reboot the KSX II. **Required**

   Once FIPS mode is activated, 'FIPS Mode: Enabled' will be displayed in the Device Information section in the left panel of the screen.

For additional security, you can also create a new Certificate Signing Request once FIPS mode is activated. This will be created using the required key ciphers. Upload the certificate after it is signed or create a self-signed certificate. The SSL Certificate status will updated from 'Not FIPS Mode Compliant' to 'FIPS Mode Compliant'.

When FIPS mode is activated, key files cannot be downloaded or uploaded.   The most recently created CSR will be associated internally with the key file. Further, the SSL Certificate from the CA and its private key are not included in the full restore of the backed-up file. The key cannot be exported from KSX II.

FIPS 140-2 Support Requirements

The KSX II supports the use of FIPS 140-20 approved encryption algorithms. This allows an SSL server and client to successfully negotiate the cipher suite used for the encrypted session when a client is configured for FIPS 140-2 only mode.

Following are the recommendations for using FIPS 140-2 with the KSX II:

KSX II

- Set the Encryption & Share to Auto on the Security Settings page. See Encryption & Share.

Microsoft Client

- FIPS 140-2 should be enabled on the client computer and in Internet Explorer.

▶ **To enable FIPS 140-2 on a Windows client:**

1. Select Control Panel > Administrative Tools > Local Security Policy to open the Local Security Settings dialog.

2. From the navigation tree, select Select Local Policies > Security Options.

3. Enable "System Cryptography: Use FIPS compliant algorithms for encryption, hashing and signing".

4. Reboot the client computer.

▶ **To enable FIPS 140-2 in Internet Explorer:**

1. In Internet Explorer, select Tools > Internet Options and click on the Advanced tab.

2. Select the Use TLS 1.0 checkbox.

3. Restart the browser.

Configuring IP Access Control

Using IP access control, you can control access to your KSX II. By setting a global Access Control List (ACL) you are ensuring that your device does not respond to packets being sent from disallowed IP addresses. The IP access control is global, affecting the KSX II as a whole, but you can also control access to your device at the group level. See Group-Based IP ACL (Access Control List) for more information about group-level control.

Important: IP address 127.0.0.1 is used by the KSX II local port. When creating an IP Access Control list, 127.0.0.1 should not be within the range of IP addresses that are blocked or you will not have access to the KSX II local port.

► **To use IP access control:**

1. Open the IP Access Control page by selecting Security > IP Access Control. The IP Access Control page opens.

2. Select the Enable IP Access Control checkbox to enable IP access control and the remaining fields on the page.

3. Choose the Default Policy. This is the action taken for IP addresses that are not within the ranges you specify.

   - Accept - IP addresses are allowed access to the KSX II device.

   - Drop - IP addresses are denied access to the KSX II device.

   Note: Both IPv4 and IPv6 addresses are supported.

► **To add (append) rules:**

1. Type the IP address and subnet mask in the IPv4/Mask or IPv6/Prefix Length field.

   Note: The IP address should be entered using CIDR (Classless Inter-Domain Routing notation, in which the first 24 bits are used as a network address).

2. Choose the Policy from the drop-down list.

3. Click Append. The rule is added to the bottom of the rules list.

► **To insert a rule:**

1. Type a rule #. A rule # is required when using the Insert command.

2. Type the IP address and subnet mask in the IPv4/Mask or IPv6/Prefix Length field.

3. Choose the Policy from the drop-down list.

4. Click Insert. If the rule # you just typed equals an existing rule #, the new rule is placed ahead of the exiting rule and all rules are moved down in the list.

Tip: The rule numbers allow you to have more control over the order in which the rules are created.

► **To replace a rule:**

1. Specify the rule # you want to replace.
2. Type the IP address and subnet mask in the IPv4/Mask or IPv6/Prefix Length field.
3. Choose the Policy from the drop-down list.
4. Click Replace. Your new rule replaces the original rule with the same rule #.

► **To delete a rule:**

1. Specify the rule # you want to delete.
2. Click Delete.
3. You are prompted to confirm the deletion. Click OK.

Home > Security > IP Access Control

IP Access Control

☑ **Enable IP Access Control**

Default policy
ACCEPT

Rule #	IPv4/Mask or IPv6/Prefix Length	Policy
1	192.168.59.192/32	ACCEPT
2	192.168.61.0/24	ACCEPT
3	255.255.0.0/16	ACCEPT

ACCEPT

Append | Insert | Replace | Delete

OK | Reset To Defaults | Cancel

SSL Certificates

The KSX II uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. When establishing a connection, the KSX II has to identify itself to a client using a cryptographic certificate.

It is possible to generate a Certificate Signing Request (CSR) and install a certificate signed by the Certificate Authority (CA) on the KSX II. The CA verifies the identity of the originator of the CSR. The CA then returns a certificate containing its signature to the originator. The certificate, bearing the signature of the well-known CA, is used to vouch for the identity of the presenter of the certificate.

▶ **To create and install a SSL certificate:**

1. Select Security > SSL Certificate.

2. Complete the following fields:

    a. Common name - The network name of the KSX II once it is installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the KSX II with a web browser but without the prefix "http://". In case the name given here and the actual network name differ, the browser will pop up a security warning when the KSX II is accessed using HTTPS.

    b. Organizational unit - This field is used for specifying to which department within an organization the KSX II belongs.

    c. Organization - The name of the organization to which the KSX II belongs.

    d. Locality/City - The city where the organization is located.

    e. State/Province - The state or province where the organization is located.

    f. Country (ISO code) - The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the U.S.

    g. Challenge Password - Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). The minimum length of this password is four characters.

    h. Confirm Challenge Password - Confirmation of the Challenge Password.

    i. Email - The email address of a contact person that is responsible for the KSX II and its security.

j.   Key length - The length of the generated key in bits. 1024 is the default.

k.   Select the Create a Self-Signed Certificate checkbox (if applicable).

3.   Click Create to generate the Certificate Signing Request (CSR).

▶   **To download a CSR certificate:**

1.   The CSR and the file containing the private key used when generating it can be downloaded by click the Download button.

   Note: The CSR and the private key file are a matched set and should be treated accordingly. If the signed certificate is not matched with the private key used to generate the original CSR, the certificate will not be useful. This applies to uploading and downloading the CSR and private key files.

2.   Send the saved CSR to a CA for certification. You will get the new certificate from the CA.

▶   **To upload a CSR:**

1.   Upload the certificate to the KSX II by clicking the Upload button.

   Note: The CSR and the private key file are a matched set and should be treated accordingly. If the signed certificate is not matched with the private key used to generate the original CSR, the certificate will not be useful. This applies to uploading and downloading the CSR and private key files.

After completing these three steps the KSX II has its own certificate that is used for identifying the card to its clients.

Important: If you destroy the CSR on the KSX II there is no way to get it back! In case you deleted it by mistake, you have to repeat the three steps as described above. To avoid this, use the download function so you will have a copy of the CSR and its private key.

Security Banner
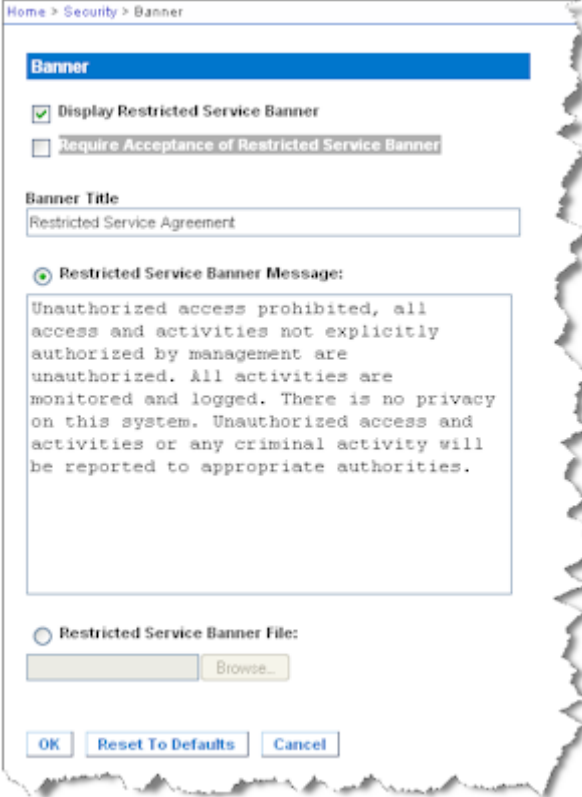
KSX II provides you with the ability to add a security banner to the KSX II login process. This feature requires users to either accept or decline a security agreement before they can access the KSX II. The information provided in a security banner will be displayed in a Restricted Service Agreement dialog after users access KSX II using their login credentials.

The security banner heading and wording can be customized, or the default text can be used. Additionally, the security banner can be configured to require that a user accepts the security agreement before they are able to access the KSX II or it can just be displayed following the login process. If the accept or decline feature is enabled, the user's selection is logged in the audit log.

▶ To configure a security banner:

1. Click Security >   Banner to open the Banner page.

2. Select Display Restricted Service Banner to enable the feature.

3. If you want to require users to acknowledge the banner prior to continuing the login process, select Require Acceptance of Restricted Service Banner. In order to acknowledge the banner, users will select a checkbox. If you do not enable this setting, the security banner will only be displayed after the user logs in and will not require users acknowledge it.

4. If needed, change the banner title. This information will be displayed to users as part of the banner. Up to 64 characters can be used.

5. Edit the information in the Restricted Services Banner Message text box. Up to 6000 characters can be entered or uploaded from a text file. To do this, do one of the following:

   a. Edit the text by manually typing in the text box. Click OK.

   b. Upload the information from .txt file by selecting the Restricted Services Banner File radio button and using the Browse feature to locate and upload the file. Click OK. Once the file is uploaded, the text from the file will appear in the Restricted Services Banner Message text box.

Note: You cannot upload a text file from the local port.

Home > Security > Banner

Banner

☑ **Display Restricted Service Banner**

☐ Require Acceptance of Restricted Service Banner

Banner Title

Restricted Service Agreement

⦿ **Restricted Service Banner Message:**

Unauthorized access prohibited, all
access and activities not explicitly
authorized by management are
unauthorized. All activities are
monitored and logged. There is no privacy
on this system. Unauthorized access and
activities or any criminal activity will
be reported to appropriate authorities.

○ **Restricted Service Banner File:**

[ ] Browse...

OK   Reset To Defaults   Cancel

Chapter 10 Maintenance

In This Chapter

Maintenance Features (Local/Remote Console)

Use:	To:	Local	Remote
Audit Log	View Dominion KSX II events sorted by date and time.	✓	✓
Device Information	View information about the Dominion KSX II and its CIMs.	✓	✓
Backup/Restore	Backup and restore the KSX II configuration.		✓
USB Profile Management	Upload custom profiles provided by Raritan tech support.		✓
CIM Firmware Upgrade	Upgrade your CIMs using the firmware versions stored in the Dominion KSX II memory.	✓	✓
Firmware Upgrade	Upgrade your Dominion KSX II firmware.		✓
Factory Reset	Perform a factory reset.	✓	
Upgrade History	View information about the latest upgrade performed.	✓	✓
Reboot	Reboot the KSX II.	✓	✓

Audit Log

A log is created of the KSX II system events.

▶ **To view the audit log for your KSX II:**

1. Choose Maintenance > Audit Log. The Audit Log page opens.

   The Audit Log page displays events by date and time (most recent events listed first). The Audit Log provides the following information:

   ▪ Date - The date and time that the event occurred based on a 24-hour clock.

   ▪ Event - The event name as listed in the Event Management page.

   ▪ Description - Detailed description of the event.

▶ **To save the audit log:**

Note: Saving the audit log is available only on the KSX II Remote Console, not on the Local Console.

1. Click Save to File. A Save File dialog appears.

2. Choose the desired file name and location and click Save. The audit log is saved locally on your client machine with the name and location specified.

▶ **To page through the audit log:**

• Use the [Older] and [Newer] links.

Device Information

The Device Information page provides detailed information about your KSX II device and the CIMs in use. This information is helpful should you need to contact Raritan Technical Support.

▶ **To view information about your Dominion KSX II and CIMs:**

- Choose Maintenance > Device Information. The Device Information page opens.

The following information is provided about the KSX II:

- Model
- Hardware Revision
- Firmware Version
- Serial Number
- MAC Address

The following information is provided about the CIMs in use:

- Port (number)
- Name
- Type (of CIM, Power Strip, or VM)
- Firmware Version
- Serial Number

Device Information

Model:	DKSX2_188
Hardware Revision:	0x60
Firmware Version:	2.3.0.5.50
Serial Number:	AE17500013
MAC Address:	00:0d:5d:03:5d:0c

CIM Information

▲ Port	Name	Type	Firmware Version	Serial Numl
3	Blade_Chassis_Port3	Dual-VM	3A80	PQ2040315(

Backup and Restore

From the Backup/Restore page, you can backup and restore the settings and configuration for your KSX II.

In addition to using backup and restore for business continuity purposes, you can use this feature as a time-saving mechanism. For instance, you can quickly provide access to your team from another KSX II by backing up the user configuration settings from the KSX II in use and restoring those configurations to the new KSX II. You can also set up one KSX II and copy its configuration to multiple KSX II devices.

▶ **To access the Backup/Restore page:**

- Choose Maintenance > Backup/Restore. The Backup/Restore page opens.

Home > Maintenance > Backup / Restore

Backup / Restore

- ⦿ Full Restore
- ○ Protected Restore
- ○ Custom Restore
  - ☐ User and Group Restore
  - ☐ Device Settings Restore

Restore File

[   ] [Browse...]

[**Backup**] [**Cancel**]

Note: Backups are always complete system backups. Restores can be complete or partial depending on your selection.

▶ **If you are using Firefox® or Internet Explorer® 5 or lower, to backup your KSX II:**

1. Click Backup. A File Download dialog appears.

2. Click Save. A Save As dialog appears.

3. Choose the location, specify a file name, and click Save. A Download Complete dialog appears.

4. Click Close. The backup file is saved locally on your client machine with the name and location specified.

> **If you are using Internet Explorer 6 or higher, to backup your KSX II:**

1. Click Backup. A File Download dialog appears that contains an Open button. Do not click Open.

   In IE 6 and higher, IE is used as the default application to open files, so you are prompted to open the file versus save the file. To avoid this, you must change the default application that is used to open files to WordPad®.

2. To do this:

   a. Save the backup file. The backup file is saved locally on your client machine with the name and location specified.

   b. Once saved, locate the file and right-click on it. Select properties.

   c. In general tab, click Change and select WordPad.

> **To restore your KSX II:**

WARNING: Exercise caution when restoring your KSX II to an earlier version. Usernames and password in place at the time of the backup will be restored. If you do not remember the old administrative usernames and passwords, you will be locked out of the KSX II.

In addition, if you used a different IP address at the time of the backup, that IP address will be restored as well. If the configuration uses DHCP, you may want to perform this operation only when you have access to the local port to check the IP address after the update.

1. Choose the type of restore you want to run:

- Full Restore - A complete restore of the entire system. Generally used for traditional backup and restore purposes.

- Protected Restore - Everything is restored except device-specific information such as IP address, name, and so forth. With this option, you can setup one KSX II and copy the configuration to multiple KSX II devices.

- Custom Restore - With this option, you can select User and Group Restore, Device Settings Restore, or both:

  - User and Group Restore - This option includes only user and group information. This option *does not* restore the certificate and the private key files. Use this option to quickly set up users on a different KSX II.

  - Device Settings Restore - This option includes only device settings such as power associations, USB profiles, blade chassis related configuration parameters, and Port Group assignments. Use this option to quickly copy the device information.

1. Click Browse. A Choose File dialog appears.

2. Navigate to and select the appropriate backup file and click Open. The selected file is listed in the Restore File field.

3. Click Restore. The configuration (based on the type of restore selected) is restored.

USB Profile Management

From the USB Profile Management page, you can upload custom profiles provided by Raritan tech support.   These profiles are designed to address the needs of your target server's configuration, in the event that the set of standard profiles does not already address them.   Raritan tech support will provide the custom profile and work with you to verify the solution for your target server's specific needs.

▶ **To access the USB Profile Management page:**

- Choose > Maintenance > USB Profile Management. The USB Profile Management page opens.

▶ **To upload a custom profile to your KSX II:**

1. Click the Browse button. A Choose File dialog appears.

2. Navigate to and select the appropriate custom profile file and click Open.   The file selected is listed in the USB Profile File field.

3. Click Upload. The custom profile will be uploaded and displayed in the Profile table.

Note: If an error or warning is displayed during the upload process (for example. overwriting an existing custom profile), you may continue with the upload by clicking Upload or cancel it by clicking on Cancel.

▶ **To delete a custom profile to your KSX II:**

1. Check the box corresponding to the row of the table containing the custom profile to be deleted.

2. Click Delete. The custom profile will be deleted and removed from the Profile table.

As noted, you may delete a custom profile from the system while it is still designated as an active profile.   Doing so will terminate any virtual media sessions that were in place.

Handling Conflicts in Profile Names

A naming conflict between custom and standard USB profiles may occur when a firmware upgrade is performed. This may occur if a custom profile that has been created and incorporated into the list of standard profiles has the same name as a new USB profile that is downloaded as part of the firmware upgrade.

Should this occur, the preexisting custom profile will be tagged as 'old_'. For example, if a custom profile called GenericUSBProfile5 has been created and a profile with the same name is downloaded during a firmware upgrade, the existing file will then be called 'old_GenericUSBProfile5'.

You can delete the existing profile if needed. See **USB Profile Management** (on page 210) for more information.

Upgrading CIMs

Use this procedure to upgrade CIMs using the firmware versions stored in the memory of your KSX II device. In general, all CIMs are upgraded when you upgrade the device firmware using the Firmware Upgrade page.

In order to make use of USB profiles, you must use a D2CIM-VUSB or D2CIM-DVUSB with updated firmware. A VM-CIM that has not had its firmware upgraded will support a broad range of configurations (Windows®, Keyboard, Mouse, CD-ROM, and Removable Device) but will not be able to make use of profiles optimized for particular target configurations. Given this, existing VM-CIMs should be upgraded with the latest firmware in order to access USB profiles. Until existing VM-CIMs are upgraded, they will be able to provide functionality equivalent to the 'Generic' profile.

Note: Only D2CIM-VUSB can be upgraded from this page.

▶ **To upgrade CIMs using the KSX II memory:**

1. Choose Maintenance > CIM Firmware Upgrade. The CIM Upgrade from page opens.

   The Port (number), Name, Type, Current CIM Version, and Upgrade CIM Version are displayed for easy identification of the CIMs.

2. Check the Selected checkbox for each CIM you want to upgrade.

   Tip: Use the Select All and Deselect All buttons to quickly select all (or deselect all) of the CIMs.

3. Click the Upgrade button. You are prompted to confirm the upgrade.

4. Click OK to continue the upgrade. Progress bars are displayed during the upgrade. Upgrading takes approximately 2 minutes or less per CIM.

Upgrading Firmware

Use the Firmware Upgrade page to upgrade the firmware for your KSX II and all attached CIMs. This page is available in the KSX II Remote Console only.

Important: Do not turn off your KSX II or disconnect CIMs while the upgrade is in progress - doing so will likely result in damage to the device or CIMs.

▶ **To upgrade your KSX II:**

1. Locate the appropriate Raritan firmware distribution file (*.RFP), found on the Raritan Firmware Upgrades webpage: http://www.raritan.com/support/firmwareupgrades and download the file.

2. Unzip the file. Read all instructions included in the firmware ZIP files carefully before upgrading.

3. Copy the firmware update file to a local PC before uploading. Do not load the file from a network drive.

4. Choose Maintenance > Firmware Upgrade. The Firmware Upgrade page opens.

5. Click the Browse button to navigate to the directory where you unzipped the upgrade file.

6. Select the "Review CIM Version Information?" checkbox if you would like information displayed about the versions of the CIMs in use.

7. Click Upload from the Firmware Upgrade page. Information about the upgrade and version numbers is displayed (if you opted to review CIM information, that information is displayed as well).

Note: At this point, connected users are logged off and new login attempts are blocked.

8. Click Upgrade and wait for the upgrade to complete. Status information and progress bars are displayed during the upgrade. Upon completion of the upgrade, the device reboots (1 beep sounds to signal the reboot).

Firmware Upgrade in Progress...

CIMs on Device Shan-KSX2 are being upgraded. It may take up to 2 minutes to upgrade the selected CIMs. Do not turn off the unit or remove CIMs until the upgrade is complete.

Progress: 0 of 1 CIMs upgraded

0%

9. As prompted, close the browser and wait approximately 5 minutes before logging on to the KSX II again.
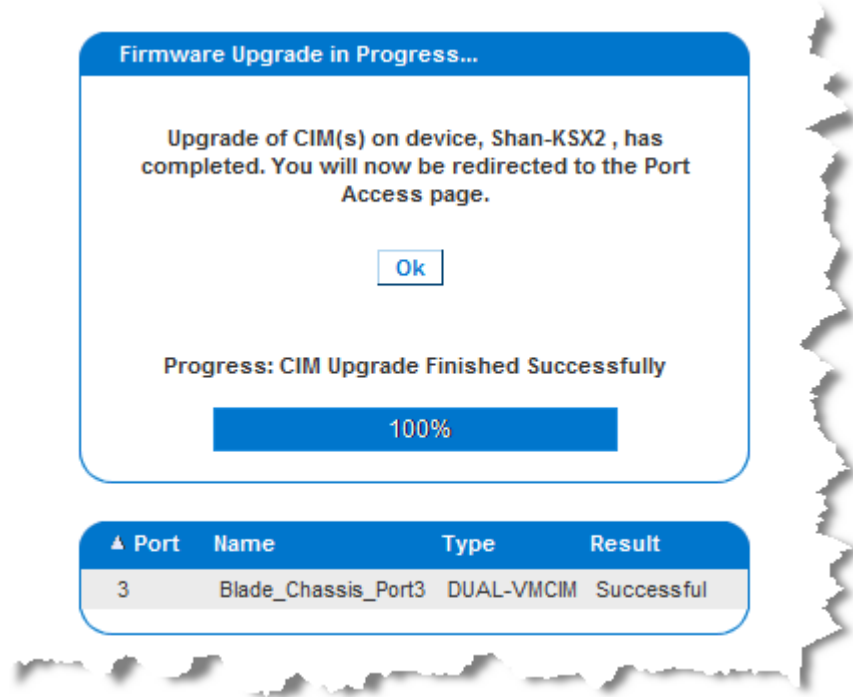
Upgrade History

The KSX II provides information about upgrades performed on the KSX II and attached CIMS.

▶ **To view the upgrade history:**

• Choose Maintenance > Upgrade History. The Upgrade History page opens.

Information is provided about the KSX II upgrade(s) that have been run, the final status of the upgrade, the start and end times, and the previous and current firmware versions. Information is also provided about the CIMS, which can be obtained by clicking the show link for an upgrade. The CIM information provided is:

- Port - The port where the CIM is connected.
- Name - The name of the CIM.
- Type - The type of CIM.
- Previous Version - Previous version of the CIM.
- Upgrade Version - Current version of the CIM.
- Result - The result of the upgrade (success or fail).
-

Rebooting

The Reboot page provides a safe and controlled way to reboot your KSX II. This is the recommended method for rebooting.

Important: All KVM and serial connections will be closed and all users will be logged off.

► **To reboot your KSX II:**

1. Choose Maintenance > Reboot. The Reboot page opens.
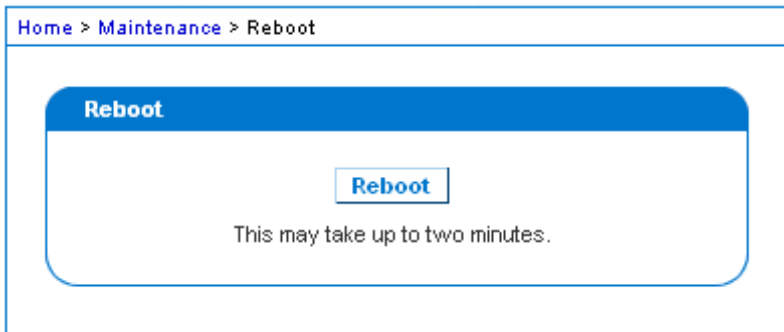
2. Click Reboot. You are prompted to confirm the action. Click Yes to proceed with the reboot.
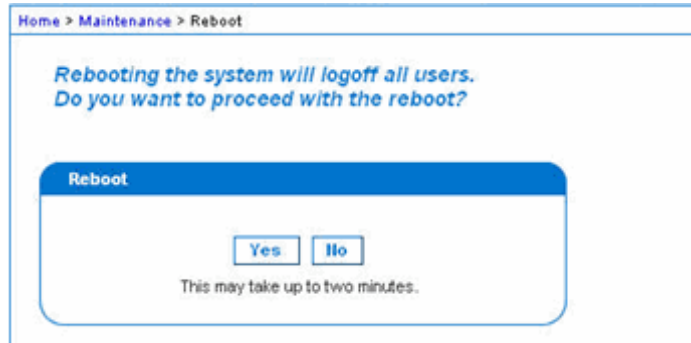
CC Unmanage

When a KSX II device is under CommandCenter Secure Gateway control and you attempt to access the device directly using the KSX II Remote Console, the following message appears (after entry of a valid user name and password).

Stopping CC-SG Management

While the KSX II is under CC-SG management, if you try to access the device directly, you are notified that it the device is under CC-SG management.

If you are managing the KSX II through CC-SG and connectivity between CC-SG and the KSX II is lost after the specified timeout interval (typically 10 minutes), you are able to end the CC-SG management session from the KSX II console.

Note: You must have the appropriate permissions to end CC-SG management of the KSX II. Additionally, the Stop CC-SG Management option will not be provided unless you are currently using CC-SG to manage the KSX II.

▶ **To stop CC-SG management of a KSX II:**

1. Click Maintenance > Stop CC-SG Management. A message indicating that the device is being managed by CC-SG will be displayed. An option to remove the device from CC-SG management will also be displayed.
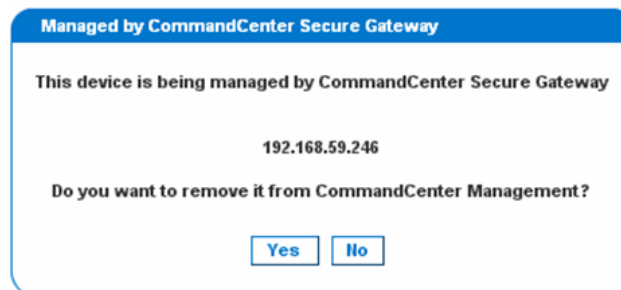
2. Click Yes to begin the processing of removing the device from CC-SG management. A confirmation message will then displayed asking you to confirm that you want the remove the device from CC-SG management.
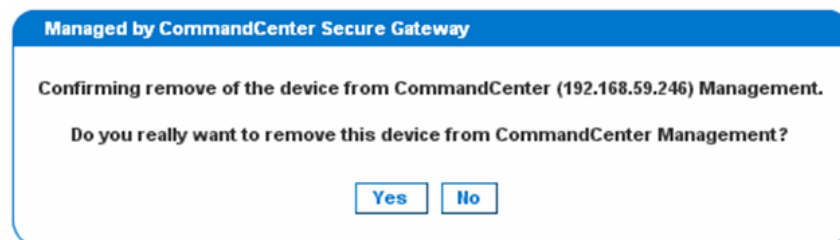
3. Click Yes to remove the device CC-SG management. Once CC-SG management has ended, a confirmation will be displayed.

Managed by CommandCenter Secure Gateway

Stop CC-SG Management is successful. The device is no longer under CC-SG Management mode.

Ok

Chapter 11 Diagnostics

The Diagnostics pages are used for troubleshooting and are intended primarily for the administrator of the KSX II device. All of the Diagnostics pages (except Device Diagnostics) run standard networking commands and the information that is displayed is the output of those commands. The Diagnostics menu options help you debug and configure the network settings.

The Device Diagnostics option is intended for use in conjunction with Raritan Technical Support.

In This Chapter

Network Interface Page

The KSX II provides information about the status of your network interface.

▶ **To view information about your network interface:**

- Choose Diagnostics > Network Interface. The Network Interface page opens.

The following information is displayed:

- Whether the Ethernet interface is up or down.
- Whether the gateway is pingable or not.
- The LAN port that is currently active.

▶ **To refresh this information:**

- Click the Refresh button.

Network Statistics Page

The KSX II provides statistics about your network interface.

▶ **To view statistics about your network interface:**

1. Choose Diagnostics > Network Statistics. The Network Statistics page opens.
2. Choose the appropriate option from the Options drop-down list:

▪ Statistics - Produces a page similar to the one displayed here.

▪ Interfaces - Produces a page similar to the one displayed here.
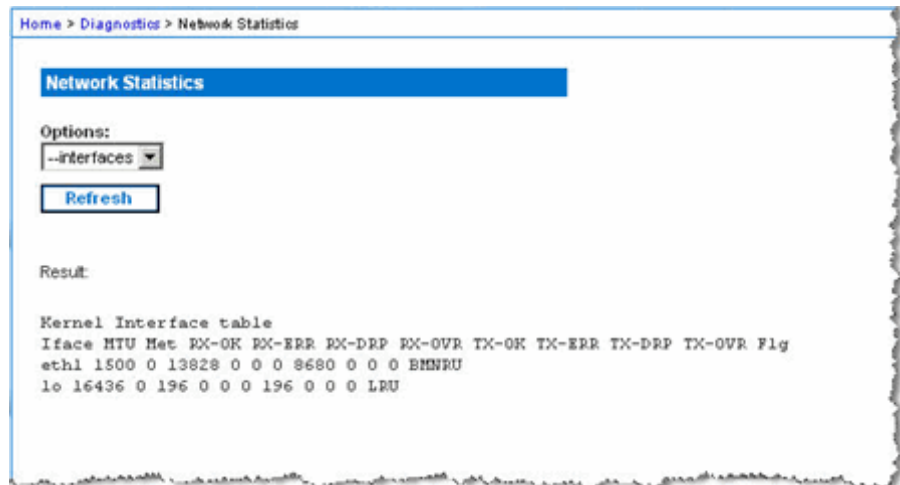
▪ Route - Produces a page similar to the one displayed here.
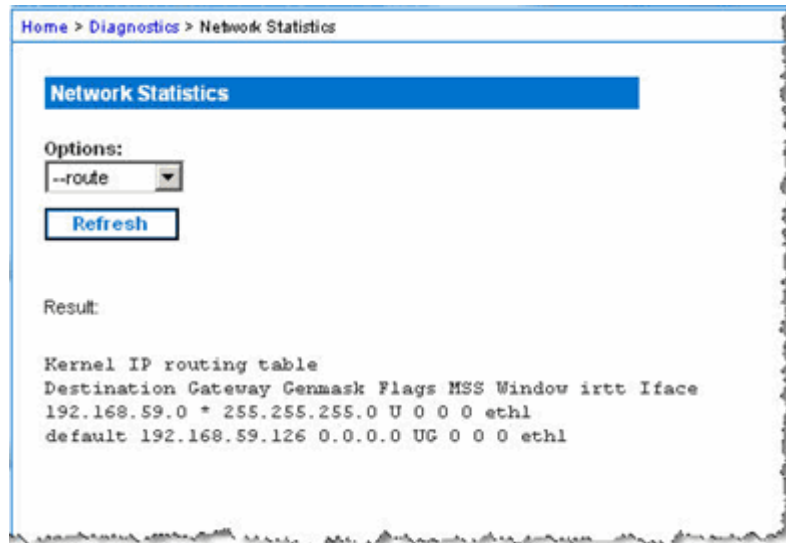
3. Click Refresh. The relevant information is displayed in the Result field.

Ping Host Page

Ping is a network tool used to test whether a particular host or IP address is reachable across an IP network. Using the Ping Host page, you can determine if a target server or another KSX II is accessible.

▶ **To ping the host:**

1. Choose Diagnostics > Ping Host. The Ping Host page opens.

2. Type either the hostname or IP address into the Hostname or IP Address field.

3. Click Ping. The results of the ping are displayed in the Result field.

Trace Route to Host Page

Trace route is a network tool used to determine the route taken to the provided hostname or IP address.

▶   **To trace the route to the host:**

1. Choose Diagnostics > Trace Route to Host. The Trace Route to Host page opens.

2. Type either the IP address or host name into the IP Address/Host Name field.

    Note: The host name cannot exceed 232 characters in length.

3. Choose the maximum hops from the drop-down list (5 to 50 in increments of 5).

4. Click Trace Route. The trace route command is executed for the given hostname or IP address and the maximum hops. The output of trace route is displayed in the Result field.

Home > Diagnostics > Trace Route to Host

Trace Route to Host

IP Address/Host Name
192.168.59.173

Maximum Hops:
10 ▾

Trace Route

Result:

traceroute started wait for 2mins....
traceroute to 192.168.59.173 (192.168.59.173), 10 hops max, 40 byte packets
1 192.168.59.173 (192.168.59.173) 0.497 ms 0.308 ms 0.323 ms
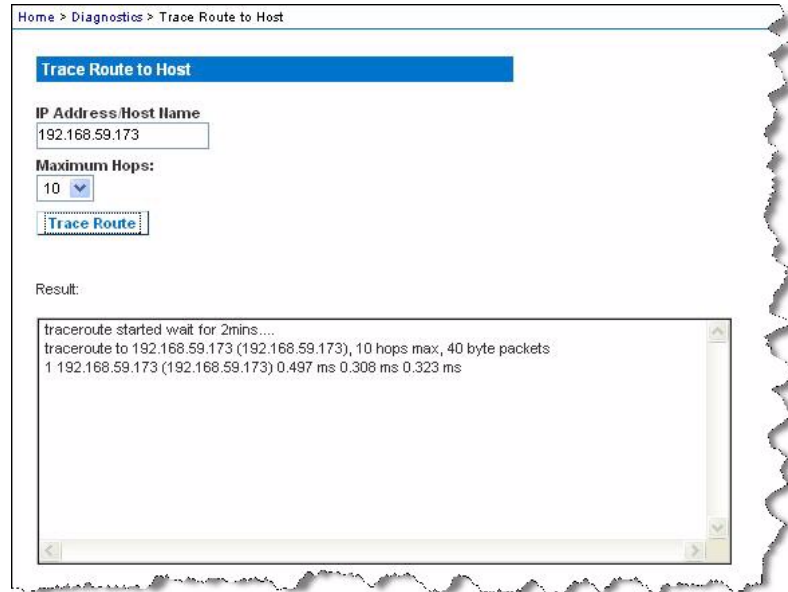
Device Diagnostics

Note: This page is for use by Raritan field engineers or when you are directed by Raritan Technical Support.

Device Diagnostics downloads the diagnostics information from KSX II to the client machine. Two operations can be performed on this page:

Operation	Description
Diagnostics Scripts	Execute a special script provided by Raritan Technical Support during a critical error debugging session. The script is uploaded to the device and executed. Once this script has been executed, you can download the diagnostics messages through the Save to File button.
Device Diagnostic Log	Download the snapshot of diagnostics messages from the KSX II to the client. This encrypted file is then sent to Raritan Technical Support; only Raritan can interpret this file.

Note: This page is accessible only by users with administrative privileges.

▶ **To run the KSX II system diagnostics:**

1. Choose Diagnostics > Device Diagnostics. The Device Diagnostics page opens.

2. To execute a diagnostics script file emailed to you from Raritan Technical Support:

   a. Retrieve the diagnostics file supplied by Raritan and unzip as necessary.

   b. Use the Browse button. A Choose File dialog appears.

   c. Navigate to and select this diagnostics file.

   d. Click Open. The file is displayed in the Script File field:

   e. Click Run Script.

   f. Send this file to Raritan Technical Support using step 4.

3. To create a diagnostics file to send to Raritan Technical Support:

   a. Click the Save to File button. The File Download dialog appears.
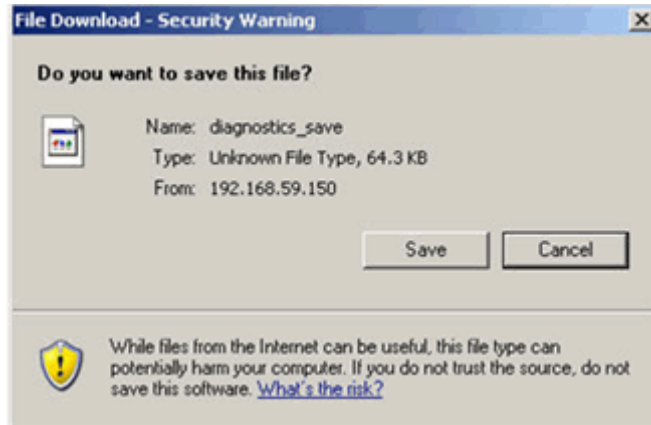
   b. Click Save. The Save As dialog appears.

   c. Navigate to the desired directory and click Save.

4. Email this file as directed by Raritan Technical Support.

Chapter 12   Command Line Interface (CLI)

Overview

The KSX II Serial Console supports all serial devices such as:

- Servers, including Windows Server 2003® when using the Emergency Management Console (EMS-) Special Administration Console, or SAC with BIOS redirection in the server BIOS.

- Routers

- Layer 2 switches

- Firewalls

- Rack PDUs (power strips)

- Other user equipment

The KSX II allows an administrator or user to access, control, and manage multiple serial devices. You can use the Command Line Interface (CLI) to configure the KSX II or to connect to target devices. The RS-232 interface may operate at all standard rates from 1200 bps to 115.2 kbps. The default settings are 9600 bps, 8 data bits, no parity bit, one stop bit, and no flow control.

The following figures describe an overview of the CLI commands. See **CLI Commands** (on page 234) for a list of all the commands, which include definitions and links to the sections in this chapter that give examples of these commands.
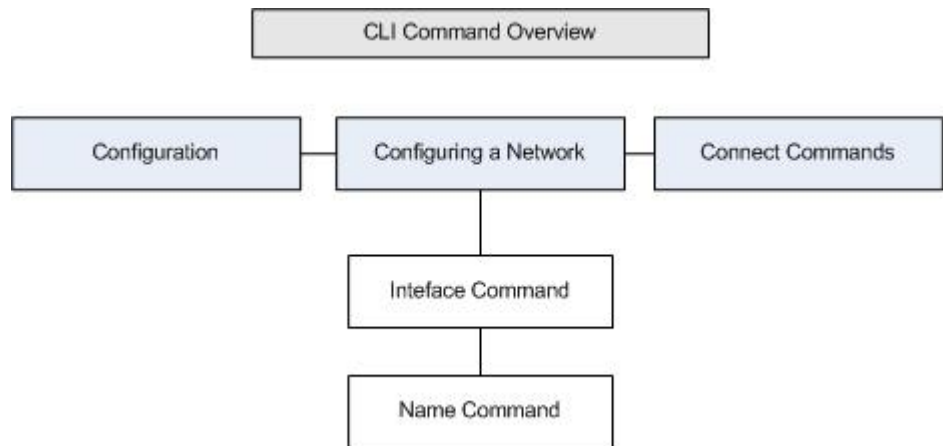
The following common commands can be used from all levels of the CLI to the preceding figure: top, history, log off, quit, show, and help.

Accessing the KSX II Using CLI

Access the KSX II by using one of the following methods:

- Telnet via IP connection
- SSH (Secure Shell) via IP connection
- Local Port-via RS-232 serial interface

A number of SSH/Telnet clients are available and can be obtained from the following locations:

- Putty - *http://www.chiark.greenend.org.uk/~sgtatham/putty/ http://www.chiark.greenend.org.uk/~sgtatham/putty/*
- SSH Client from ssh.com - *www.ssh.com http://www.ssh.com*
- Applet SSH Client - *www.netspace.org/ssh http://www.netspace.org/ssh*
- OpenSSH Client - *www.openssh.org http://www.openssh.org*

SSH Connection to the KSX II

Use any SSH client that supports SSHv2 to connect to the KSX II. You must enable SSH access from the Devices Services page.

Note: For security reasons, SSH V1 connections are not supported by the KSX II.

SSH Access from a Windows PC

▶ **To open an SSH session from a Windows® PC:**

1. Launch the SSH client software.
2. Enter the IP address of the KSX II server. For example, 192.168.0.192.
3. Choose SSH, which uses the default configuration port 22.
4. Click Open.

The login as: prompt appears.

SSH Access from a UNIX/Linux Workstation

▶ **To open an SSH session from a UNIX®/Linux® workstation and log in as the user admin, enter the following command:**

```
ssh –l admin 192.168.30.222
```

The Password prompt appears.

Telnet Connection to the KSX II

Due to the lack of security, user name, password and all traffic is in clear-text on the wire. Telnet access is disabled by default.

Enabling Telnet

If you wish to use Telnet to access the KSX II, first access the KSX II from the CLI or a browser.

▶ **To enable Telnet:**

1. Select Device Settings > Device Services and then select the Enable TELNET Access checkbox.

2. Enter the Telnet port.

3. Click OK.

Once Telnet access is enabled, you can use it to access the KSX II and set up the remaining parameters.

Accessing Telnet from a Windows PC

▶ **To open a Telnet session from a Windows® PC:**

1. Choose Startup > Run.

2. Type *Telnet* in the Open text box.

3. Click OK. The Telnet page opens.

4. At the prompt enter the following command: `Microsoft Telnet> open <IP address>` where <IP address> is the KSX II IP address.

5. Press the Enter key. The following message appears: `Connecting To <IP address>... The login as` prompt appears.

Local Serial Port Connection to the KSX II

The local serial port of the KSX II must be connected to the COM port of a computer system, a terminal, or some other serial capable device using a null modem cable with DB-9F null on both ends.

If your KSX II's terminal port uses an RJ45 jack, a special cable (CRLVR) is used with an ASCSDB9F connector on the client machine. The CRLVR may also be used if RJ45-RJ45 connection to local port is established - that is, if you connect the local port of a KSX II device as a serial target to another KSX II.

Port Settings

Ensure that the port settings (serial communication parameters) are configured as follows:

- Data bits = 8
- Parity = None
- Stop bits =1
- Flow Control = None
- Bits per second = 9600

Logging On

▶ **To log in, enter the user name admin as shown:**

1. Log in as `admin`

2. The Password prompt appears. Enter the default password: *raritan*

   The welcome message displays. You are now logged on as an administrator.

After reviewing the following **Navigation of the CLI** (on page 231) section, perform the Initial Configuration tasks.

```
Welcome!

192.168.59.202 login: admin

Passwd:

-----------------------------------------------------
---------------------------

Device Type: Dominion KSX2     Model: DKSX2_188

Device Name: YongKSX2          FW Version: 1.0.0.5.6321
SN: AE17950009

IP Address:  192.168.59.202    Idle Timeout: 0min

IP Address:  192.168.59.202    Idle Timeout: 0min

Port Port                 Port        Port   Port

No.  Name                 Type        Status
Availability

1  - Dominion_KSX2_Port1 Not Available down   idle

2  - Dominion_KSX2_Port3 Not Available down   idle

3  - Dominion_KSX2_Port4 Not Available down   idle

4  - Dominion_KSX2_Port5 Not Available down   idle

5  - YongFedora7         VM             up     idle

6  - Yong-Laptop-XP     Not Available down   idle

7  - Dominion_KSX2_Port8 Not Available down   idle

8  - Serial Port 1      Serial        up    idle

9  - Serial Port 2      Serial        up    idle

10 - Serial Port 3      Serial        up    idle

11 - Serial Port 4      Serial        up    idle

12 - Serial Port 5      Serial        up    idle

13 - Serial Port 6      Serial        up    idle

14 - Serial Port 7      Serial        up    idle

15 - Serial Port 8      Serial        up    idle

Current Time: Tue Dec 04 13:22:17 2007

admin >
```

```
login as: Janet

Password:

Authentication successful.


-----------------------------------------------------
------------

Welcome to the KSX II  [Model: KSX2]

UnitName:KSX II      FirmwareVersion:3.0.0.5.1
Serial:WACEA00008

IP Address:192.168.51.194  UserIdletimeout:99min

-----------------------------------------------------
-------------

Port Port                      Port Port

No.  Name                      No.  Name

1 - Port1 [U]                   2 - Port2 [U]

3 - Port3 [U]                   4 - Port4 [U]

Current Time: Wed Sep 20 16:05:50 2006

Janet >
```

Navigation of the CLI

Before using the CLI, it is important to understand CLI navigation and syntax. There are also some keystroke combinations that simplify CLI use.

Completion of Commands

The CLI supports the completion of partially-entered commands. After entering the first few characters of an entry, press the Tab key. If the characters form a unique match, the CLI will complete the entry.

- If no match is found, the CLI displays the valid entries for that level.
- If multiple matches are found, the CLI displays all valid entries.

Enter additional text to make the entry unique and press the Tab key to complete the entry.

CLI Syntax -Tips and Shortcuts

Tips

- Commands are listed in alphabetical order.

- Commands are not case sensitive.

- Parameter names are single word without underscore.

- Commands without arguments default to show current settings for the command.

- Typing a question mark (?) after a command produces help for that command.

- A pipe symbol (|) indicates a choice within an optional or required set of keywords or arguments.

Shortcuts

- Press the Up arrow key to display the last entry.

- Press Backspace to delete the last character typed.

- Press Ctrl + C to terminate a command or cancel a command if you typed the wrong parameters.

- Press Enter to execute the command.

- Press Tab to complete a command. For example, `Admin Port > Conf.` The system then displays the `Admin Port > Config >` prompt.

Common Commands for All Command Line Interface Levels

Following are the commands that are available at all CLI levels. These commands also help navigate through the CLI.

Commands	Description
top	Return to the top level of the CLI hierarchy, or the "username" prompt.
history	Display the last 200 commands the user entered into the KSX II CLI.
help	Display an overview of the CLI syntax.
quit	Places the user back one level.
logout	Logs out the user session.

Initial Configuration Using CLI

Note: These steps, which use the CLI, are optional since the same configuration can be done via KVM. See Getting Started for more information.

KSX II devices come from the factory with default factory settings. When you first power up and connect to the device, you must set the following basic parameters so the device can be accessed securely from the network:

1. Reset the administrator password. All KSX II devices are shipped with the same default password. Therefore, to avoid security breaches it is imperative that you change the admin password from raritan to one customized for the administrators who will manage the KSX II device.

2. Assign the IP address, subnet mask, and gateway IP address to allow remote access.

Setting Parameters

To set parameters, you must be logged on with administrative privileges. At the top level, you will see the `"Username" >` prompt, which for the initial configuration is `"admin"`. Enter the top command to return to the top menu level.

Note: If you have logged on with a different user name, that user name will appear instead of admin.

Setting Network Parameters

Network parameters are configured using the interface command.

```
admin > Config > Network > interface ipauto none ip
192.168.151.12 mask 255.255.255.0 gw 192.168.151.1 mode
auto
```

When the command is accepted, the device automatically drops the connection. You must reconnect to the device using the new IP address and the user name and password you created in the resetting factory default password section.

Important: If the password is forgotten, the KSX II will need to be reset to the factory default from the Reset button on the back of the KSX II. The initial configuration tasks will need to be performed again if this is done.

The KSX II now has the basic configuration and can be accessed remotely via SSH, GUI, or locally using the local serial port. The administrator needs to configure the users and groups, services, security, and serial ports to which the serial targets are attached to the KSX II.

CLI Prompts

The Command Line Interface prompt indicates the current command level. The root portion of the prompt is the login name. For a direct admin serial port connection with a terminal emulation application, Admin Port is the root portion of a command.

```
admin >
```

For TELNET/SSH, admin is the root portion of the command:

```
admin > config > network >
```

0

CLI Commands

The table below lists and describes all available CLI commands.

Command	Description
config	Port configuration command Switch to the Configuration menu.
connect	Connect to a port.
diagnostics	Switch to diagnostic commands menu.
help	Display an overview of the CLI syntax.
history	Display the current session's command line history.
interface	Configure the KSX II network interface.
listports	List accessible ports.
logout	Logout of the current CLI session.
name	Display or change a device name and/or the hostname.
quit	Return to previous command
userlist	List users.

Security Issues

Elements to consider when addressing security for console servers:

- Encrypting the data traffic sent between the operator console and the KSX II device.
- Providing authentication and authorization for users.
- Security profile.

The KSX II supports each of these elements; however, they must be configured prior to general use.

Target Connections and the CLI

The purpose of the KSX II is to let authorized users establish connections to various targeted devices using the connect command. Before connecting to a target, the terminal emulation and escape sequence must be configured. When a target is disconnected, the appropriate disconnect message appears. The KSX II also provides the ability to share ports among users.

Setting Emulation on a Target

▶ **To set emulation on the target:**

- Ensure that the encoding in use on the host matches the encoding configured for the target device, that is, if the character-set setting on a Sun™ Solaris™ server is set to ISO8859-1, the target device should also be set to ISO8859-1.

  Note: ISO9660 format is the standard supported by Raritan. However, other CD-ROM extensions may also work.

- Ensure that the terminal emulation on the target host connected to the KSX II serial port is set to VT100, VT220, VT320 or ANSI.

On most UNIX® systems, export TERM=vt100 (or vt220|vt320|ansi)" sets the preferred terminal emulation type on the UNIX target device, that is, if the terminal type setting on a HP-UX® server is set to VT100, the Access Client should also be set to VT100.

The setting for terminal emulation on the KSX II is a property associated with the port settings for a particular target device. Ensure that the settings for terminal emulation in the client software such as Telnet or SSH client are capable of supporting the target device.

Port Sharing Using CLI

It is possible for access client users to share ports with other authenticated and authorized users, regardless of whether they are access client users (RSC) or SSH/Telnet users. Port sharing is used for training or for troubleshooting applications.

- Users are notified in real time if they have Write access or Read-Only access at any point during the port-sharing session.
- Users who have Write permissions can request Write access to a port.

Administering the KSX II Console Server Configuration Commands

Note: CLI commands are the same for SSH, Telnet, and Local Port access sessions.

The Network command can be accessed in the Configuration menu for the KSX II.

Configuring Network

The network menu commands are used to configure the KSX II network adapter.

Commands	Description
interface	Configure the KSX II device network interface.
name	Network name configuration
ipv6	Set/get IPv6 network parameters.

Interface Command

The Interface command is used to configure the KSX II network interface. The syntax of the interface command is:

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask
<subnetmask>] [gw <ipaddress>] [mode <mode>]

Set/Get ethernet parameters

ipauto <none|dhcp> IP auto configuration (none/dhcp)

ip <ipaddress> IP Address

mask <subnetmask> Subnet Mask

gw <ipaddress> Gateway IP Address

mode <mode> Set Ehternet Mode
(auto/10hdx/10fdx/100hdx/100fdx/1000fdx)
```

Interface Command Example

The following command enables the interface number 1, sets the IP address, mask, and gateway addresses, and sets the mode to auto detect.

```
Admin > Config > Network > interface ipauto none ip
192.16.151.12 mask 255.255.255.0 gw 192.168.51.12 mode
auto
```

Note: Both IPv4 and IPv6 addresses are supported.

Name   Command

The name command is used to configure the network name. The syntax of the name is:

```
name [devicename <devicename>] [hostname <hostname>]
```

Device name configuration

```
devicename <devicename>   Device Name

hostname  <hostname>    Preferred host name (DHCP
only)
```

Name Command Example

The following command sets the network name:

```
Admin > Config > Network > name devicename My-KSX2
```

Connect Commands

The connect commands provide a means to access ports and their history.

Command	Description
connect	Connect to a port. The port sub-menu, reached using escape key sequence.
clearhistory	Clear history buffer for this port. Only available to users who have Write access.
clientlist	Display all users on the port.
close	Close this target connection.
gethistory	Display the history buffer for this port. Not available to users who only have Read-Only permissions.
getwrite	Get write access for the port. Not available to users who only have Read-Only permissions.
help	Display an overview of the commands.
history	Display the current session's command line history.
powerstatus	Quersy the Power Status port. Not available to users who do not have power permission.
powertoggle	Toggle power on and off for the port. Not available to users who do not have power permission. Operational for power associated serial targets only.
quit	Close this target connection.
return	Return to the target session.
sendbreak	Send a break to the connected target. Not available to users who only have Read-Only permissions.
writelock	Lock write access to this port. Not available to users who only have Read-Only permissions.
writeunlock	Unlock write access to this port. Not available to users who only have Read-Only permissions.

IPv6 Command

Use the IPv6_command to set IPv6 network parameters and retrieve existing IPv6 parameters.

Chapter 13 KSX II Local Console

In This Chapter

Overview

The KSX II provides at-the-rack access and administration via its local port, which features a browser-based graphical user interface for quick, convenient switching between servers. The KSX II Local Console provides a direct analog connection to your connected servers; the performance is as if you were directly connected to the server's keyboard, mouse, and video ports. The KSX II Local Console provides the same administrative functionality as the KSX II Remote Console.

Using the KSX II Local Console

Simultaneous Users

The KSX II Local Console provides an independent access path to the connected KVM target servers. For serial connections, the access path is shared. Using the Local Console does not prevent other users from simultaneously connecting over the network. And even when remote users are connected to KSX II, you can still simultaneously access your servers from the rack via the Local Console.

KSX II Local Console Interface

When you are located at the server rack, the KSX II provides standard KVM management and administration via the KSX II Local Console. The KSX II Local Console provides a direct KVM (analog) connection to your connected servers; the performance is exactly as if you were directly connected to the server's keyboard, mouse, and video ports. Additionally, the KSX II provides terminal emulation when accessing serial targets.

There are many similarities among the KSX II Local Console and the KSX II Remote Console graphical user interfaces. Where there are differences, they are noted in the help.

The KSX II Local Console Factory Reset option is available in the KSX II Local Console but not the KSX II Remote Console.

Security and Authentication

In order to use the KSX II Local Console, you must first authenticate with a valid username and password. The KSX II provides a fully-integrated authentication and security scheme, whether your access is via the network or the local port. In either case, the KSX II allows access only to those servers to which a user has access permissions. See User Management for additional information on specifying server access and security settings.

If your KSX II has been configured for external authentication services (LDAP/LDAPS, RADIUS, or Active Directory), authentication attempts at the Local Console also are authenticated against the external authentication service.

Note: You can also specify no authentication for Local Console access; this option is recommended only for secure environments.

▶ **To use the KSX II Local Console:**

1. Connect a keyboard, mouse, and video display to the local ports at the back of the KSX II.

2. Start the KSX II. The KSX II Local Console interface displays.

Local Console Smart Card Access

To use a smart card to access a server at the Local Console, plug a USB smart card reader into the KSX II using one of the USB ports located on the KSX II. Once a smart card reader is plugged in or unplugged from the KSX II, the KSX II autodetects it. For a list of supported smart cards and additional system requirements, see **Supported and Unsupported Smart Card Readers** (on page 282) and **Minimum System Requirements** (on page 283).

When mounted onto the target server, the card reader and smart card will cause the server to behave as if they had been directly attached. Removal of the smart card or smart card reader will cause the user session to be locked or you will be logged out depending on how the card removal policy has been setup on the target server OS. When the KVM session is terminated, either because it has been closed or because you switch to a new target, the smart card reader will be automatically unmounted from the target server.

▶ **To mount a smart card reader onto a target via the KSX II Local console:**

1. Plug a USB smart card reader into the KSX II using one of the USB ports located on the device. Once attached, the smart card reader will be detected by the KSX II.

2. From the Local Console, click Tools.

3. Select the smart card reader from the Card Readers Detected list. Select None from the list if you do not want a smart card reader mounted.

4. Click OK. Once the smart card reader is added, a message will appear on the page indicating you have completed the operation successfully. A status of either Selected or Not Selected will appear in the left panel of the page under Card Reader.

▶ **To update the Card Readers Detected list:**

- Click Refresh if a new smart card has been mounted. The Card Readers Detected list will be refreshed to reflect the newly added smart card reader.

Select Card Reader

Card Readers Detected

None

USB SmartCard Reader (Gemplus)

OK   Refresh   Cancel
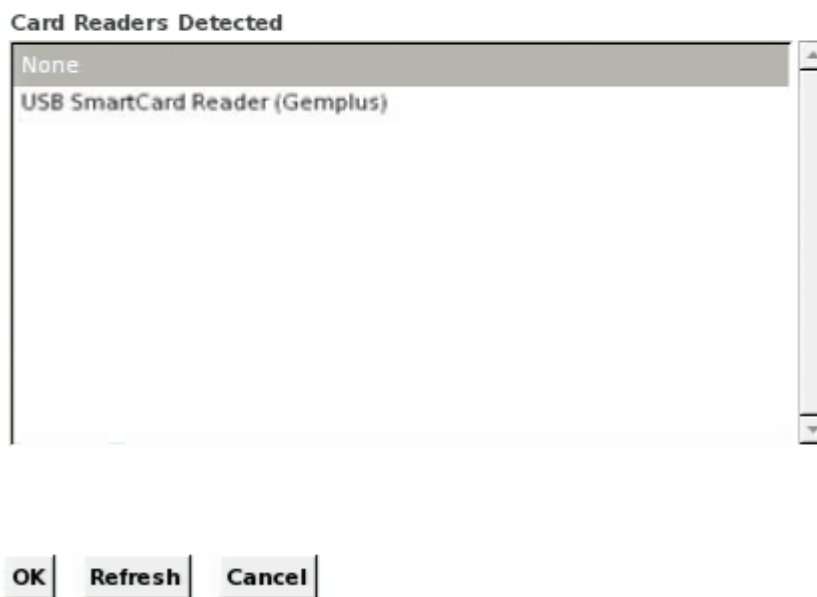
Local Console USB Profile Options

From the USB Profile Options section of the Tools page, you can choose from the available USB profiles for a local port.

The ports that can be assigned profiles are displayed in the Port Name field and the profiles that are available for a port appear in the Select Profile To Use field after the port is selected. The profiles selected for use with a port appear in the Profile In Use field.

▶ **To apply a USB profile to a local console port:**

1. In the Port Name field, select the port you want to apply the USB profile to.

2. In the Select Profile To Use field, select the profile to use from among those available for the port.

243

3. Click OK. The USB profile will be applied to the local port and will appear in the Profile In Use field.
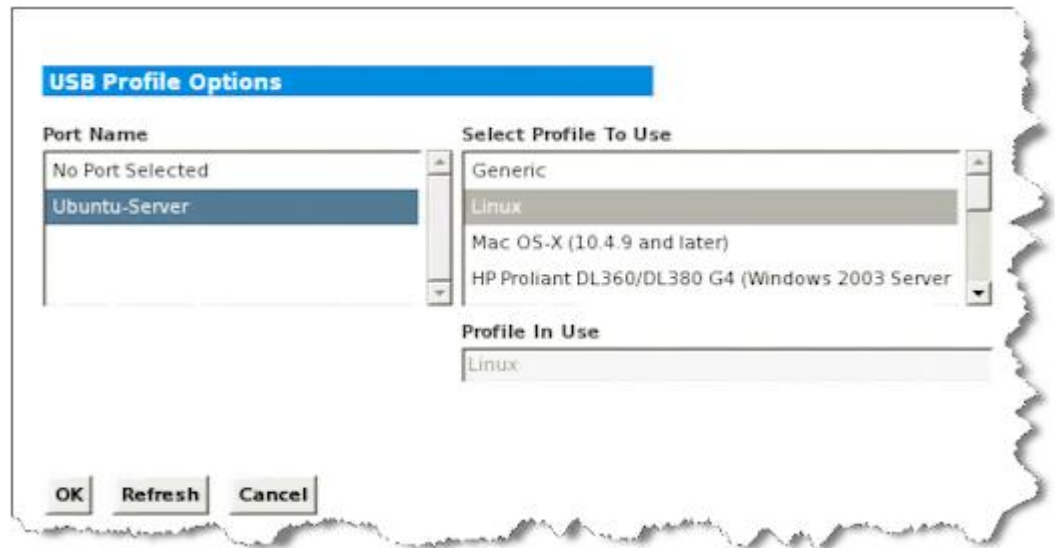
Available Resolutions

The KSX II Local Console provides the following resolutions to support various monitors:

*   800x600
*   1024x768
*   1280x1024

Each of these resolutions supports a refresh rate of 60Hz and 75Hz.

Port Access Page (Local Console Server Display)

After you login to the KSX II Local Console, the Port Access page opens. This page lists all of the KSX II ports, the connected KVM target servers, and their status and availability.

Also displayed on the Port Access page are blade chassis that have been configured in the KSX II.

The blade chassis is displayed in an expandable, hierarchical list on the Port Access page, with the blade chassis at the root of the hierarchy and the individual blades labeled and displayed below the root. Use the Expand Arrow icon next to the root chassis to display the individual blades.

Note: To view the blade chassis in a hierarchal order, blade-chassis subtypes must be configured for the blade server chassis.

By default, the View by Port tab will be displayed on the Port Access page. The View by Group tab displays port groups and can be expandable to display ports that are assigned to the port group.

▶ **To use the Port Access page:**

1. Log in to the Local Console.

   The KVM target servers are initially sorted by Port Number. You can change the display to sort on any of the columns.

   - Port Number - Numbered from 1 to the total number of ports available for the KSX II device.

   - Port Name - The name of the KSX II port. Initially, this is set to Dominion-KX2-Port# but you can change the name to something more descriptive. When you click a Port Name link, the Port Action Menu appears.

   Note: Do not use apostrophes for the Port (CIM) Name.

   - Status - The status for standard servers is either up or down.

   - Type - The type of server or CIM. For blade chassis, the type can be Blade Chassis, Blade, BladeChassisAdmin, and BladeChassisURL.

   - Availability - The Availability can be Idle, Connected, Busy, or Unavailable. Blade servers will have an availability of either shared or exclusive when a connection to that blade is in place.

2. Click View by Port or View by Group to switch between views.

   - In addition to the Port Number, Port Name, Status, Type, and Availability, a Group column is also displayed on the View by Group tab. This column contains the port groups that are available.

3. Click the Port Name of the target server you want to access. The Port Action Menu appears. See **Port Action Menu** (on page 46) for details on available menu options.

4. Choose the desired menu command from the Port Action Menu.

▶ **To change the display sort order:**

- Click the column heading by which you want to sort. The list of KVM target servers is sorted by that column.

Server Display

After you login to the KSX II Local Console, the Port Access page opens. This page lists all of the KSX II ports, KVM target servers and serial servers, and their status and availability.

Port Access

Click on the individual port name to see allowable operations.
0 of 1 Remote KVM channels currently in use.

▲ Port Number	Port Name	Port Type	Status	Availability
1	Win Target	VM	up	idle
2	Dominion_KSX2_Port2	Not Available	down	idle
3	Dominion_KSX2_Port3	Not Available	down	idle
4	KSX-G2 Admin	VM	up	idle
5	Dominion_KSX2_Port5	Not Available	down	idle
6	Dominion_KSX2_Port6	Not Available	down	idle
7	Dominion_KSX2_Port7	Not Available	down	idle
8	Dominion_KSX2_Port8	Not Available	down	idle
9	Cisco 2501	Serial	up	idle
10	SP-2	Serial	up	idle
11	Serial Port 3	Serial	up	idle
12	Serial Port 4	Serial	up	idle
13	SP - 5	Serial	up	idle
14	Serial Port 6	Serial	up	idle
15	Serial Port 7	Serial	up	idle
16	Serial Port 8	Serial	up	idle

The KVM and serial target servers are initially sorted by Port Number; you can change the display to sort on any of the columns.

- Port Number - Numbered from 1 to the total number of ports available for the KSX II.

- Port Name - The name of the KSX II port. Initially this is set to Dominion-KSX II-Port#, but you can change the name to something more descriptive. When you click the Port Name link, an Action Menu is opened.

- Port Type - Serial, KVM, Power Strip, or Not Available.

Note: Do not use apostrophes for the Port (CIM) Name.

- Status - The Status is either up or down.

  ▶ **To change the sort order:**
  - Click the column heading you want to sort by. The list of KVM target servers is sorted by that column.

Hot Keys and Connect Keys

Because the KSX II Local Console interface is completely replaced by the interface for the target server you are accessing, a hot key is used to disconnect from a target and return to the local port GUI. A connect key is used to connect to a target or switch between targets.

The Local Port hot key allows you to rapidly access the KSX II Local Console user interface when a target server is currently being viewed. The default is to press the Scroll Lock key twice in rapid succession, but you can designate another key combination (available in the Local Port Settings page) as the hot key. See *KSX II Local Console Local Port Settings* (on page 251) for more information.

Connect Key Examples

Standard servers

Connect key action	Key sequence example
Access a port from the local port GUI	Access port 5 from the local port GUI: • Press Left ALT > Press and Release 5 > Release Left ALT
Switch between ports	Switch from target port 5 to port 11: • Press Left ALT > Press and Release 1 > Press and Release 1 > Release Left ALT
Disconnect from a target and return to the local port GUI	Disconnect from target port 11 and return to the local port GUI (the page from which you connected to target): • Double Click Scroll Lock

Blade chassis

Connect key action	Key sequence example
Access a port from the local port GUI	Access port 5, slot 2: • Press Left ALT > Press and Release 5 > Press and Release - > Press and Release 2 > Release Left ALT

Blade chassis	
Connect key action	**Key sequence example**
Switch between ports	Switch from target port 5, slot 2 to port 5, slot 11: • Press Left ALT > Press and Release 5 > Press and Release - > Press and Release 1 > Press and Release 1 > Release Left ALT
Disconnect from a target and return to the local port GUI	Disconnect from target port 5, slot 11 and return to the local port GUI (the page from which you connected to target): • Double Click Scroll Lock

Supported Keyboard Languages

The KSX II provides keyboard support for the languages listed in the following table.

Note: You can use the keyboard for Chinese, Japanese, and Korean for display only; local language input is not supported at this time for the KSX II Local Console functions. For more information about non-US keyboards, see Informational Notes.

Note: Raritan strongly recommends that you use system-config-keyboard to change languages if you are working in a Linux environment.

Language	Regions	Keyboard layout
US English	United States of America and most of English-speaking countries: for example, Canada, Australia, and New Zealand.	US Keyboard layout
US English International	United States of America and most of English-speaking countries: for example, Netherlands	US Keyboard layout
UK English	United Kingdom	UK layout keyboard
Chinese Traditional	Hong Kong S. A. R., Republic of China (Taiwan)	Chinese Traditional
Chinese Simplified	Mainland of the People's Republic of China	Chinese Simplified
Korean	South Korea	Dubeolsik Hangul

Language	Regions	Keyboard layout
Japanese	Japan	JIS Keyboard
French	France	French (AZERTY) layout keyboard.
German	Germany and Austria	German keyboard (QWERTZ layout)
Belgian	Belgium	Belgian
Norwegian	Norway	Norwegian
Danish	Denmark	Danish
Swedish	Sweden	Swedish
Hungarian	Hungary	Hungarian
Slovenian	Slovenia	Slovenian
Italian	Italy	Italian
Spanish	Spain and most Spanish speaking countries	Spanish
Portuguese	Portugal	Portuguese

Special Sun Key Combinations

The following key combinations for Sun™ Microsystems server's special keys operate on the local port. These special are available from the Keyboard menu when you connect to a Sun target server:

Sun key	Local port key combination
Again	Ctrl+ Alt +F2
Props	Ctrl + Alt +F3
Undo	Ctrl + Alt +F4
Stop A	Break a
Front	Ctrl + Alt + F5
Copy	Ctrl + Alt + F6
Open	Ctrl + Alt + F7
Find	Ctrl + Alt + F9
Cut	Ctrl + Alt + F10
Paste	Ctrl + Alt + F8
Mute	Ctrl + Alt + F12

Sun key	Local port key combination
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol -	Ctrl + Alt + KPAD -
Stop	No key combination
Power	No key combination

Accessing a Target Server

▶ **To access a target server:**

1. Click the Port Name of the target you want to access. The Port Action Menu is displayed.

2. Choose Connect from the Port Action menu. The video display switches to the target server interface.

Returning to the KSX II Local Console Interface

Important: The KSX II Local Console default hot key is to press the Scroll Lock key twice rapidly. This key combination can be changed in the Local Port Settings page. See *KSX II Local Console Local Port Settings* (on page 251).

▶ **To return to the KSX II Local Console from the target server:**

- Press the hot key twice rapidly (the default hot key is Scroll Lock). The video display switches from the target server interface to the KSX II Local Console interface.

Local Port Administration

The KSX II can be managed by either the KSX II Local Console or the KSX II Remote Console. Note that the KSX II Local Console also provides access to:

- Factory Reset
- Local Port Settings

Note: Only users with administrative privileges can access these functions.

KSX II Local Console Local Port Settings

From the Local Port Settings page, you can customize many settings for the KSX II Local Console including keyboard, local port hot key, video switching delay, power save mode, local user interface resolution settings, and local user authentication.

Note: This feature is available only on the KSX II Local Console.

▶ **To configure the local port settings:**

1. Choose Device Settings > Local Port Settings. The Local Port Settings page opens.

2. Choose the appropriate keyboard type from among the options in the drop-down list:

   - US
   - US/International
   - United Kingdom
   - French (France)
   - German (Germany)
   - JIS (Japanese Industry Standard)
   - Simplified Chinese
   - Traditional Chinese
   - Dubeolsik Hangul (Korean)
   - German (Switzerland)
   - Norwegian (Norway)
   - Swedish (Sweden)
   - Danish (Denmark)
   - Belgian (Belgium)

   Note: Keyboard use for Chinese, Japanese, and Korean is for display only. Local language input is not supported at this time for KSX II Local Console functions.

3. Choose the local port hotkey. The local port hotkey is used to return to the KSX II Local Console interface when a target server interface is being viewed. The default is to Double Click Scroll Lock, but you can select any key combination from the drop-down list:

Hot key:	Take this action:
Double Click Scroll Lock	Press Scroll Lock key twice quickly
Double Click Num Lock	Press Num Lock key twice quickly

Hot key:	Take this action:
Double Click Caps Lock	Press Caps Lock key twice quickly
Double Click Left Alt key	Press the left Alt key twice quickly
Double Click Left Shift key	Press the left Shift key twice quickly
Double Click Left Ctrl key	Press the left Ctrl key twice quickly

4. Set the Video Switching Delay from between 0 - 5 seconds, if necessary. Generally 0 is used unless more time is needed (certain monitors require more time to switch the video).

5. If you would like to use the power save feature:

   a. Select the Power Save Mode checkbox.

   b. Set the amount of time (in minutes) in which Power Save Mode will be initiated.

6. Choose the resolution for the KSX II Local Console from the drop-down list:

   ▪ 800x600

   ▪ 1024x768

   ▪ 1280x1024

7. Choose the refresh rate from the drop-down list:

   ▪ 60 Hz

   ▪ 75 Hz

8. Choose the type of local user authentication:

   ▪ Local/LDAP/RADIUS. This is the recommended option. For more information about authentication, see **Remote Authentication** (on page 36).

   ▪ None. There is no authentication for Local Console access. This option is recommended for secure environments only.

9. Select the "Ignore CC managed mode on local port" checkbox if you would like local user access to the KSX II even when the device is under CC-SG management.

Note: If you initially choose not to ignore CC Manage mode on the local port but later want local port access, you will have to remove the device from under CC-SG management (from within CC-SG). You will then be able to check this checkbox.

10. Click OK.

Enable Local Ports

Note: Some changes to the Local Port Settings will restart the browser.

☑ Enable Standard Local Port

Local Port Settings

Keyboard Type
US

Local Port Hotkey   Local Port Connectkey
Double Click Scroll Lock   Disabled

Video Switching Delay (in secs)
0

☐ Power Save Mode

Power Save Mode Timeout (in minutes)
10

Resolution
1024x768

Refresh Rate (Hz)
60 Hz

Local User Authentication
◉ Local/LDAP/RADIUS
○ None
☑ Ignore CC managed mode on local port

OK   Reset To Defaults   Cancel

▶ **To reset back to defaults:**

● Click Reset to Defaults.

KSX II Local Console Factory Reset

Note: This feature is available only on the KSX II Local Console.

The KSX II offers several types of reset modes from the Local Console user interface.

*Note: It is recommended that you save the audit log prior to performing a factory reset. The audit log is deleted when a factory reset is performed and the reset event is not logged in the audit log. For more information about saving the audit log, see **Audit Log** (on page 205).*

▶ **To perform a factory reset:**

1. Choose Maintenance > Factory Reset. The Factory Reset page opens.

2. Choose the appropriate reset option from the following options:

- Full Factory Reset - Removes the entire configuration and resets the device completely to the factory defaults. Note that any management associations with CommandCenter will be broken. Because of the complete nature of this reset, you will be prompted to confirm the factory reset.

- Network Parameter Reset - Resets the network parameters of the device back to the default values (click Device Settings > Network Settings to access this information):

  - IP auto configuration

  - IP address

  - Subnet mask

  - Gateway IP address

  - Primary DNS server IP address

  - Secondary DNS server IP address

  - Discovery port

  - Bandwidth limit

  - LAN interface speed & duplex

  - Enable automatic failover

  - Ping interval (seconds)

  - Timeout (seconds)

1. Click Reset to continue. You will be prompted to confirm the factory reset because all network settings will be permanently lost.

2. Click OK button proceed. Upon completion, the KSX II device is automatically restarted.

Resetting the KSX II Using the Reset Button

On the back panel of the device, there is a Reset button. It is recessed to prevent accidental resets (you will need a pointed object to press this button).

The actions that are performed when the Reset button is pressed are defined in the graphical user interface. See Encryption & Share.

Note: It is recommended that you save the audit log prior to performing a factory reset. The audit log is deleted when a factory reset is performed and the reset event is not logged on the audit log. For more information about saving the audit log, see **Audit Log** *(on page 205).*

▶ **To reset the device:**

1. Power off the KSX II.

2. Use a pointed object to press and hold the Reset button.

3. While continuing to hold the Reset button, power the KSX II device back on.

4. Continue holding the Reset button for 10 seconds.

Once the device has been reset, two short beeps signal its completion.

Chapter 14 Modem Configuration

In This Chapter

Certified Modems for UNIX, Linux and MPC

Following is a list of modems that are certified to work for UNIX®, Linux®, and MPC:

- US Robotics Courier™ 56K Business Modem (Model# 3453B)
- Zoom/Fax Modem 56Kx Dualmode (Model# 2949)
- Zoom 56k v.92/v.90 Modem (Model # 3049)
- US Robotics v.92 56k Fax Modem (Model# 5686)
- US Robotics 56k SportSter® Modem

Low Bandwidth KVM Settings

Following are the settings that Raritan recommends in order to achieve optimum performance when using KVM over low bandwidth speeds typical of DSL connections. This information applies to both virtual KVM and MPC.

Setting	To achieve optimum performance:
Connection speed	Select Connections > Properties. Set the Connection Speed to a value that best matches the client-to-server connection. This ranges from 384 Kb (for lower DSL speeds) to >1MB.
Color depth	Select Connections > Properties. Reduce the Color Depth as far as possible. The lower this is set, the better the video refresh response on the target will be. The impact is noticeable when opening and moving folders on the target desktop. Specifically, the display is updated much quicker, improving the overall usability of the connection.
Noise filter	Select Video > Video Settings. The Noise Filter should be set to 7 (the highest value). At this setting, less bandwidth will be used for target screen changes, resulting in improved local and remote mouse synchronization.

Note: Setting the color depth to low and the noise filter to high will cause a degradation in how the video is displayed. However, this tradeoff is offset by the overall improved usability due to better mouse synchronization and video update.

Smoothing	Select Connections > Properties. Set Smoothing to high. This will improve the appearance of target video by reducing the video noise that is displayed.
Auto color calibration	Select Video > Auto-sense Video Settings Deselect the Automatic Color Calibration checkbox to disable the option.
Quick sense video mode	Select Video > Video Settings to open the Settings dialog. Select the "Quick sense video mode" radio to

Setting	To achieve optimum performance:
	enable this option.

Client Dial-Up Networking Configuration

Configuring Microsoft Windows® Dial-Up Networking for use with KSX II allows configuration of a PC to reside on the same PPP network as the KSX II. After the dial-up connection is established, connecting to a KSX II is achieved by pointing the web browser to the PPP Server IP. Modem installation guidelines are provided for the following client based systems:

- Windows 7®
- Windows XP® operating system
- Windows Vista®

Windows 2000 Dial-Up Networking Configuration

1. Choose Start > Programs > Accessories > Communications > Network and Dial-Up Connections.

2. Double-click the Make New Connection icon when the Network and Dial-Up Connections window appears.

3. Click Next and follow the steps in the Network Connection Wizard dialog to create custom dial-up network profiles.

4. Click the Dial-up to private network radio button and click Next.

5. Select the checkbox before the modem that you want to use to connect to the KSX II and then click Next.
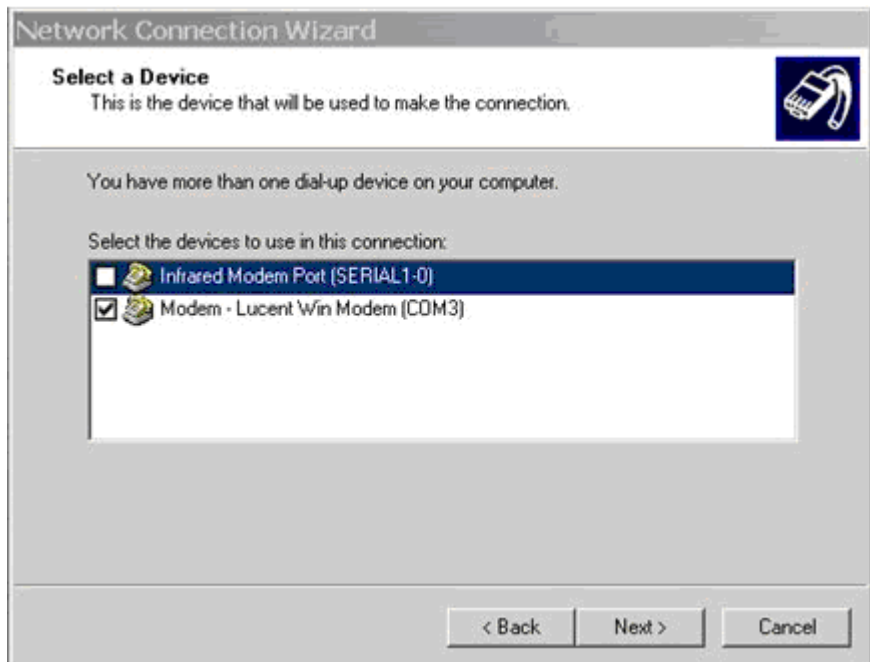
6. Type the area code and phone number you wish to dial in the appropriate fields.

7. Click the Country/region code drop-down arrow and select the country or region from the list.
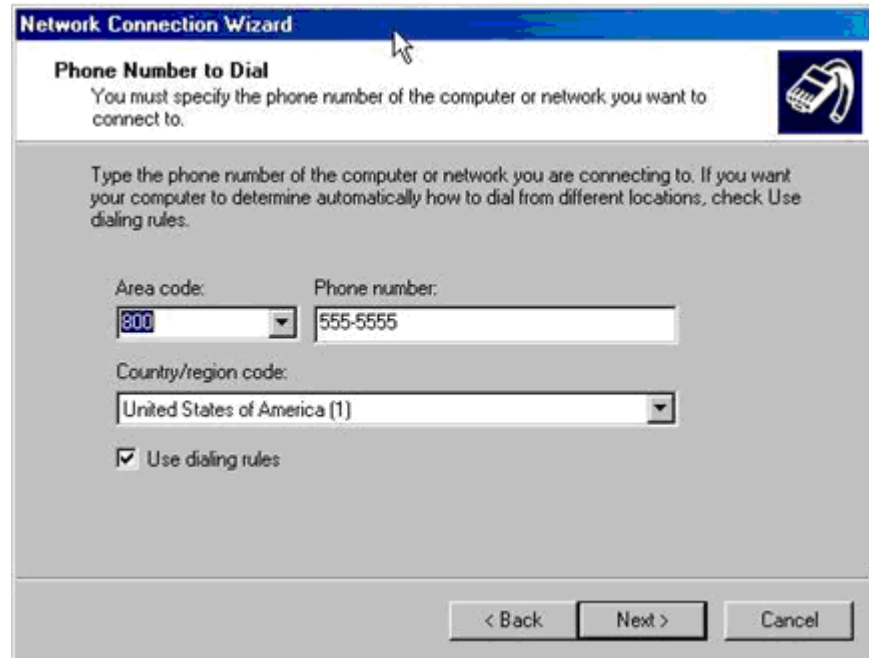
8. Click Next. The Connection Availability dialog appears.

9. Click the Only for myself radio button in the Connection Availability dialog.

10. Click Next. The Network Connection has been created.

11. Type the name of the Dial-up connection.

12. Click Finish.

13. Click Dial to connect to the remote machine when the Dial dialog appears. A dialog indicating that a successful connection has been established will appear.

Consult the Windows 2000® Dial-up Networking Help if you receive any error messages.

Windows Vista Dial-Up Networking Configuration

1. Click Start and then click Network. The Network window opens.

2. Select Network and Sharing Center at the top of the window. The Network and Sharing Center window opens.

3. Select "Set up a Connection or Network".

4. Select "Set up a dial-up connection". The "Set up a dial-up connection" dialog appears.

5. Enter the dial-up number.

6. Enter your username and password.

Note: In order to access the KSX II, the username and password cannot use a \ (backslash).
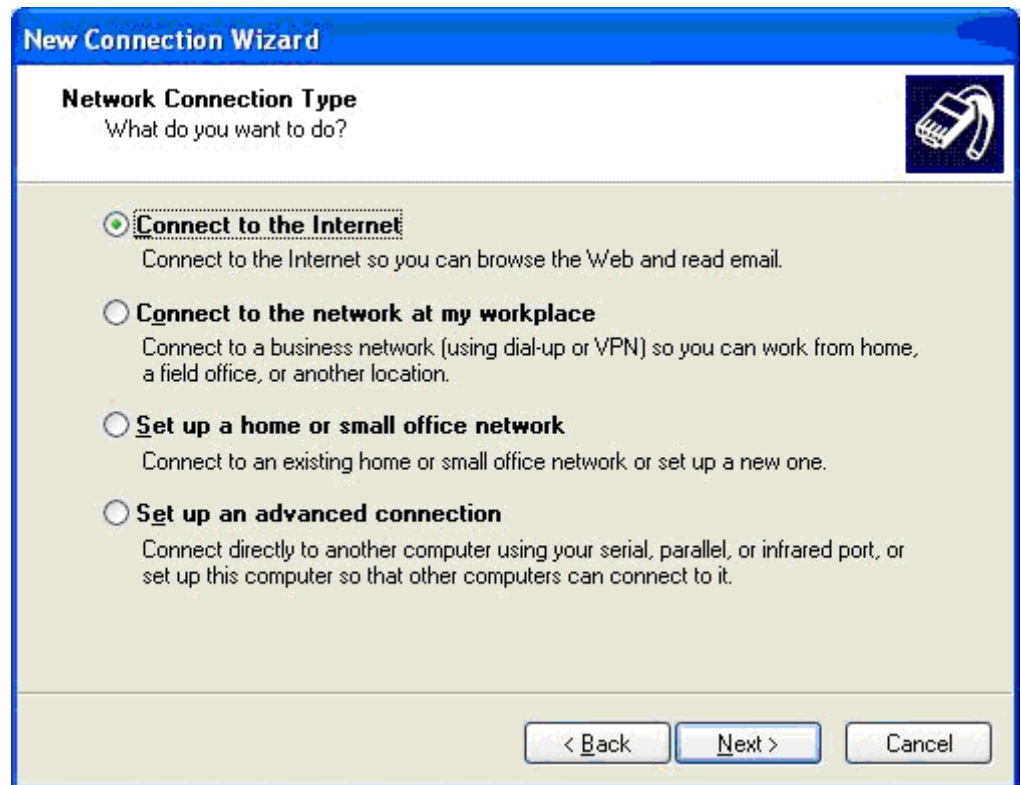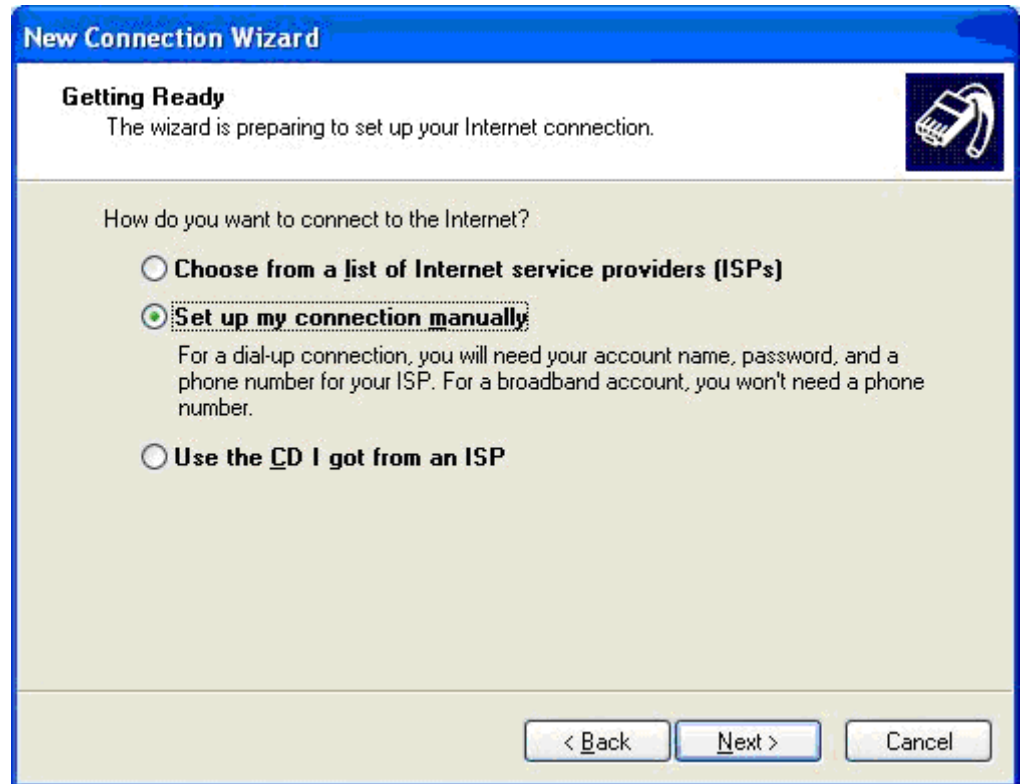
7. Click Connect.

Windows XP Dial-Up Networking Configuration

1. Choose Start > Programs > Accessories > Communications > New Connection Wizard.

2. Click Next and follow the steps in the New Connection Wizard to create custom dial-up network profiles.
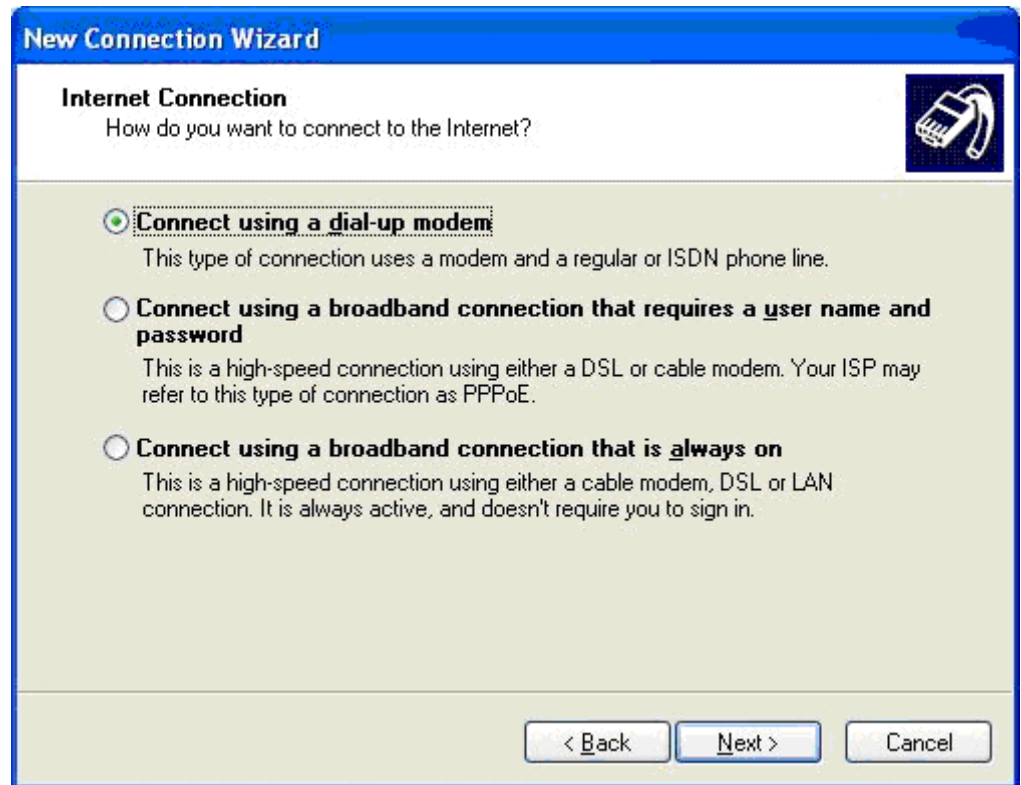
3. Click the Connect to the Internet radio button and click Next.

4. Click the "Set up my connection manually" radio button and click Next.

5. Click the "Connect using a dial-up modem" radio button and click Next.

6. Type a name to identify this particular connection in the ISP Name field and click Next.

7. Type the phone number for the connection in the Phone number field and click Next.

8. Type your ISP information. Type the user name and password in the appropriate fields, and retype the password to confirm it.

9. Select the checkbox before the appropriate option below the fields and click Next.

10. Click Finish.

11. Click Dial to connect to the remote machine when the Dial dialog appears. A dialog indicating that you connected successfully appears. If you get any errors, consult Windows XP® Dial-up Networking Help.

Note: The maximum modem speed connecting to the KSX II is 33,600 bps, as it is a Linux® default limitation.

Appendix A Specifications

In This Chapter

Physical Specifications

Part number	Line item description	UPC code	Power	Weight	Product dimensions (WxDxH)	Shipping weight	Shipping dimensions (WxDxH)
KSX2144	4 KVM and 4 Serial Port KSX II with multiple user network access and local port; virtual media.	785813650054	100/240 V 50/60 Hz 0.6A 27 Watts	8.65 lbs	1.75" x 17.3" x 11.4"	14.85 lbs	22" x 16.6" x 6.5"
				3.9kg	44mm x 439mm x 290mm	6.7 kg	559mm x 422mm x 165mm
KSX2188	8 KVM and 8 Serial Port KSX II with multiple user network access and local port; virtual media.	785813650047	100/240 V 50/60 Hz 0.6A 27 Watts	8.65 lbs	1.75" x 17.3" x 11.4"	14.85 lbs	22" x 16.6" x 6.5"
				3.9kg	44mm x 439mm x 290mm	6.7 kg	559mm x 422mm x 165mm

Supported Operating Systems (Clients)

The following operating systems are supported on the Virtual KVM Client and Multi-Platform Client (MPC):

Client operating system	Virtual media (VM) support on client
Windows 7®	Yes
Windows XP®	Yes
Windows 2008®	Yes
Windows Vista®	Yes
Windows 2000® SP4 Server	Yes
Windows 2003® Server	Yes
Windows 2008® Server	Yes
Red Hat® Desktop 5.0	Yes. Locally held ISO image, Remote File Server mounting directly from KSX II.
Red Hat Desktop 4.0	Yes. Locally held ISO image, Remote File Server mounting directly from KSX II.
Open SUSE 10, 11	Yes. Locally held ISO image, Remote File Server mounting directly from KSX II.
Fedora® 8 - 11	Yes. Locally held ISO image, Remote File Server mounting directly from KSX II.
Mac® OS	No
Solaris™	No

The JRE™ plug-in is available for the Windows® 32-bit and 64-bit operating systems. MPC and VKC can be launched only from a 32-bit browser, or 64-bit IE7 or IE8 browser.

Following are the Java™ 32-bit and 64-bit Windows operating system requirements.

Mode	Operating system	Browser
Windows x64 32-bit mode	Windows XP®	• Internet Explorer® 6.0 SP1+ or 7.0, IE 8 • Firefox® 1.06 - 3

Mode	Operating system	Browser
	Windows Server 2003®	• Internet Explorer 6.0 SP1++, IE 7, IE 8 • Firefox 1.06 - 3
	Windows Vista®	• Internet Explorer 7.0 or 8.0
	Windows 7®	• Internet Explorer 7.0 or 8.0 • Firefox 1.06 - 3
Windows x64 64-bit mode	Windows XP	64bit OS, 32bit browsers:
	Windows XP Professional®	• Internet Explorer 6.0 SP1+, 7.0 or 8.0
	Windows XP Tablet®	• Firefox 1.06 - 3
	Windows Vista	64bit mode, 64bit browsers:
	Windows Server 2003	• Internet Explorer 7.0 or 8.0
	Windows Server 2008	
	Windows 7	

Supported Operating Systems and CIMs (KVM Target Servers)

In addition to the new D2CIMs, most Dominion CIMs are supported. The following table displays the supported target server operating systems, CIMs, virtual media, and mouse modes:

Note: D2CIM-VUSB is not supported on Sun™ (Solaris™) targets.

271

Supported Dominion CIMs & D2CIMs	Operating system and serial devices (where applicable)	Virtual media	Absolute mouse mode	Intelligent mouse mode	Standard mouse mode
• DCIM-PS2 • DCIM-PS2 • DCIM-USB • DCIM-USB G2	• Windows XP® operating system • Windows 2000® operating system • Windows 2000 Server® • Windows 2003 Server® • Windows Vista® operating system			✓	✓
• D2CIM-VUSB	• Windows XP® operating system • Windows 2000® operating system • Windows 2000 Server® • Windows 2003 Server® • Windows Vista® operating system	✓		✓	✓

Target server	Supported CIMs		Mouse modes			
	Dominion DCIMs	D2CIMs	VM	AM	IM	SM
Windows XP operating system Windows 2000 operating system Windows 2000 Server® Windows 2003 Server® Windows Vista operating system			✓	✓	✓	✓
Red Hat® Enterprise Workstation 3.0,	DCIM-PS2 DCIM-USB	D2CIM-VUSB (excluding Red Hat Enterprise	✓		✓	✓

❊ Raritan.

Target server	Supported CIMs		Mouse modes				
4.0 and 5.0	DCIM-USB G2	Workstation 3.0)					
SUSE Linux Professional 9.2 and 10	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓				✓
Fedora® Core 3® and above	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓				✓
Mac OS	DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓	✓			
All Solaris OSs supported in Dominion KSX II	DCIM-SUN DCIM-SUSB DCIM-USB G2					✓	✓
IBM® AIX®	DCIM-USB DCIM-USB G2 DCIM-PS2						✓
HP UX®	DCIM-USB DCIM-USB G2 DCIM-PS2						✓
Serial Devices	Serial device support does not require a CIM					✓	

Legend:

- VM -   Virtual Media (D2CIM-VUSB only)
- AM: Absolute Mouse Synchronization (D2CIM-VUSB only)
- IM: Intelligent Mouse Mode
- SM: Standard Mouse Mode
- ✓ : Supported

The DCIM-USB G2 provides a small slide switch on the back of the CIM. Move the switch to P for PC-based USB KVM target servers; move the switch to S for Sun USB KVM target servers.
A new switch position takes effect only after the CIM is power-cycled. To power-cycle the CIM, remove the USB connector from the target server and plug it back in a few seconds later.

![Raritan logo]

273

Supported Browsers

KSX II supports the following browsers:

- Internet Explorer® 6, 7 and 8
- Firefox® 1.5, 2.0, and 3.0 (up to build 3.0.10)
- Safari®

Computer Interface Modules (CIMs)

Part number	Line item description	UPC code	Weight	Product dimensions (WxDxH)	Shipping weight	Shipping dimensions (WxDxH)
D2CIM-VUSB	KSX II Computer Interface Module [USB port with virtual media]	785813332004	0.2 lbs	1.3" x 3.0" x 0.6"	0.2 lbs	7.2" x 9" x 0.6"
DCIM-SUN	KSX II Computer Interface Module [Sun port, HD15 video]	785813338549	0.2 lbs	1.3" x 3.0" x 0.6"	0.2 lbs	7.2" x 9" x 0.6"

Supported Paragon CIMS and Configurations

The KSX II supports the P2CIM-APS2DUAL and P2CIM-AUSBDUAL CIMs, which provide two RJ45 connections to different KVM switches. Support of these CIMs provides a second path to access the target in the event that one of the KVM switches is blocked or fails.

Paragon CIM	Supports	Does not support
P2CIM-APS2DUAL	• Servers with IBM® PS/2-type keyboard and mouse ports • Automatic skew compensation (when the CIMs are connected to Paragon II, not from a KSX II) • Intelligent Mouse mode • Standard Mouse mode	• Virtual media • Smart cards • Absolute Mouse mode • Use with blade chassis • Cascaded KVM configurations
P2CIM-AUSBDUAL	• Servers with USB- or Sun™ USB-type keyboard and mouse ports • Automatic skew compensation (when the CIMs are connected to Paragon II, not from a KSX II) • Intelligent Mouse mode • Standard Mouse mode	• Virtual media • Smart cards • Absolute Mouse mode • Use with blade chassis • Cascaded KVM configurations

KSX II to KSX II Guidelines

The following system configuration guidelines should be followed when you are using Paragon CIMs in a KSX II to KSX II configuration:

Concurrent Access

Both KSX II KVM switches should be configured with the same policy for concurrent access to targets, either both PC-Share or both Private.

If Private access to targets is required, both KVM switches must be configured accordingly:

- From Security > Security Settings > Encryption & Share, set PC Share Mode to 'Private'

This guarantees that concurrent access to targets is prohibited, for all targets by all user groups.

The KSX II allows for more granular control of concurrent access to targets on a per user group basis. This is done by setting the user group's PC Share permissions.   However, this is only enforced within the boundary of a KSX II.   User Group PC Share permissions must not be relied on if Privacy must be guaranteed when using the P2CIM-APS2DUAL or P2CIM-AUSBDUAL with the KSX II.

CIM Name Updates

The P2CIM-APS2 and P2CIM-AUSB names are stored within the CIM's memory.   There are two memory locations provided to accommodate the Paragon naming convention (12 characters) and the KSX II naming convention (32 characters).

When first connected to a KSX II, the Paragon name will be retrieved from memory and written into the CIM memory location used by KSX II. Subsequent queries for the CIM name or updates to the CIM name from the KSX II will be made to the memory location used by the KSX II. Updates will not be made by the KSX II to the memory location used by Paragon II.

When the CIM name is updated by one KSX II, the other KSX II will detect and retrieve the updated name on the next attempt to connect to that target. Until that time, the name will not be updated on the other KSX II.

Port Status and Availability

The port status, displayed on the KSX II Port Access page as either Up or Down, is updated to show whether the CIM is powered up and connected to the KSX II port.

The port availability, as displayed on the KSX II Port Access page as Idle, Busy or Connected, is only updated to reflect activity on a target that has been initiated from that same KSX II.

If a connection to the target is in place from the other KSX II, the availability is checked when a connection is attempted. Access is denied or allowed consistent with the PC-Share policy in place for the KSX II. Until that time, the availability is not be updated on the other KSX II.

If access is denied because the target is busy, a notification is displayed.

Working from CC-SG

Operations initiated from CC-SG are based on the Status, Availability and CIM name reported by the managed KSX II. When the target is connected to two managed KSX IIs and the devices are added to CC-SG, two nodes will be created. Each node will have its own oob-kvm interface associated with it. Alternatively, a single node can be configured with an oob-kvm interface from each KSX II.

If the KSX IIs are configured for 'Private' mode, when a second connection is attempted the user is notified that they cannot connect and access is denied.

When a port name change is initiated via the CC-SG Port Profile pane, the changed name is pushed to the managed KSX II. The corresponding port name of the other KSX II will not be updated in CC-SG until a connection is attempted to the target port via the other KSX II's oob-kvm interface.

KSX II to Paragon II Guidelines

The P2CIM-APS2DUAL or P2CIM-AUSBDUAL can be connected to a KSX II and Paragon II.

Concurrent Access

Both the KSX II and Paragon II must be configured with the same policy for concurrent access to targets.

Paragon II operation mode	Mode description	Supported?
Private	A server or other device on a specific channel port can be accessed exclusively by only one user at a time.	Supported. Both Paragon II and the KSX II must be set to Private. The Private setting is applied on to KSX II device, not per user group. The Paragon II uses Red to indicate 'busy' or Green to indicate 'available'.

Paragon II operation mode	Mode description	Supported?
PC Share	A server or other device on a specific channel port can be selected and controlled by more than one user, but only one user has keyboard and mouse control at any one time.	Supported. However, PC Share Idle Timeout, which is configured on the Paragon II, is not supported. Both users will have concurrent keyboard and mouse control. The Paragon II uses Green to indicate 'available'. This will also be true if another user is already accessing the target.
Public View	While one user is accessing a server or other device on a specific channel port, other users can select that channel port and view the video output from that device. However, only the first user will have keyboard and mouse control until they disconnect or switch away.	Not supported. This mode cannot be used when connecting the CIM to a Paragon II and the KSX II. The Paragon II uses Yellow to indicate it is in P-View mode.

CIM Name Updates

- CIM names updated from Paragon II are stored and retrieved from the CIM memory location corresponding to the Paragon naming convention.
- CIM names updated from the KSX II are stored and retrieved from the CIM memory location corresponding to the KSX II naming convention.
- CIM name updates do not propagate between the Paragon II and the KSX II.

Supported Video Resolutions

Ensure that each target server's video resolution and refresh rate are supported by the KSX II and that the signal is noninterlaced.

Video resolution and cable length are important factors in the ability to obtain mouse synchronization. See **Target Server Connection Distance and Video Resolution** (on page 288).

The KSX II supports these resolutions:

Resolutions	
640x350 @70Hz	1024x768 @75Hz
640x350 @85Hz	1024x768 @90Hz
640x400 @56Hz	1024x768 @100Hz
640x400 @84Hz	1152x864 @60Hz
640x400 @85Hz	1152x864 @70Hz
640x480 @60Hz	1152x864 @75Hz
640x480 @66.6Hz	1152x864 @85Hz
640x480 @72Hz	1152x870 @75.1Hz
640x480 @75Hz	1152x900 @66Hz
640x480 @85Hz	1152x900 @76Hz
720x400 @70Hz	1280x720@60Hz
720x400 @84Hz	1280x960 @60Hz
720x400 @85Hz	1280x960 @85Hz
800x600 @56Hz	1280x1024 @60Hz
800x600 @60Hz	1280x1024 @75Hz
800x600 @70Hz	1280x1024 @85Hz
800x600 @72Hz	1360x768@60Hz
800x600 @75Hz	1366x768@60Hz
800x600 @85Hz	1368x768@60Hz
800x600 @90Hz	1400x1050@60Hz
800x600 @100Hz	1440x900@60Hz
832x624 @75.1Hz	1600x1200 @60Hz
1024x768 @60Hz	1680x1050@60Hz

Note: Composite Sync and Sync-on-Green video require an additional adapter.

Note: Some resolutions may not be available by default. If you do not see a resolution, plug in the monitor first, remove the monitor and then plug in the CIM.

Note: If the 1440x900 and 1680x1050 resolutions are not displayed but are supported by the target server's graphics adapter card, a DDC-1440 or DDC-1680 adapter may be required.

KSX II Local Console Support Languages

The KSX II Local Console supports the following language keyboards: US English, UK English, German, French, Japanese, Korean, Simplified Chinese, and Traditional Chinese.

Note: Keyboard use for Chinese, Japanese, and Korean is for display only; local language input is not supported at this time for KSX II Local Console functions.

TCP and UDP Ports Used

Port	Description
HTTP, Port 80	This port can be configured as needed. See ***HTTP and HTTPS Port Settings*** (on page 141). By default, all requests received by the KSX II via HTTP (port 80) are automatically forwarded to HTTPS for complete security. The KSX II responds to Port 80 for user convenience, relieving users from having to explicitly type in the URL field to access the KSX II, while still preserving complete security.
HTTPS, Port 443	This port can be configured as needed. See ***HTTP and HTTPS Port Settings*** (on page 141). By default, this port is used for multiple purposes, including the web server for the HTML client, the download of client software (MPC/VKC) onto the client's host, and the transfer of KVM and virtual media data streams to the client.
KSX II (Raritan KVM-over-IP) Protocol, Configurable Port 5000	This port is used to discover other Dominion devices and for communication between Raritan devices and systems, including CC-SG. By default, this is set to Port 5000, but you may configure it to use any TCP port not currently in use. For details on how to configure this setting, see Network Settings.
SNTP (Time Server) on Configurable UDP Port 123	The KSX II offers the optional capability to synchronize its internal clock to a central time server. This function requires the use of UDP Port 123 (the standard for SNTP), but can also be configured to use any port of your designation. **Optional**
LDAP/LDAPS on Configurable Ports 389 or 636	If the KSX II is configured to remotely authenticate user logons via the LDAP/LDAPS protocol, ports 389 or 636 will be used, but the system can also be configured to use any port of your designation. **Optional**
RADIUS on Configurable Port 1812	If the KSX II is configured to remotely authenticate user logons via the RADIUS protocol, either port 1812 will be used, but the system can also be configured to use any port of your designation. **Optional**
RADIUS Accounting on Configurable Port 1813	If the KSX II is configured to remotely authenticate user logons via the RADIUS protocol, and also employs RADIUS accounting for event logging, port 1813 or an additional port of your designation will be used to transfer log notifications.
SYSLOG on Configurable UDP Port 514	If the KSX II is configured to send messages to a Syslog server, then the indicated port(s) will be used for communication - uses UDP Port 514.
SNMP Default UDP Ports	Port 161 is used for inbound/outbound read/write SNMP access and port 162 is used for outbound traffic for SNMP traps. **Optional**
TCP Port 21	Port 21 is used for the KSX II command line interface (when you are working with Raritan Technical Support).

Smart Card Readers

Supported and Unsupported Smart Card Readers

Only USB type external smart card readers are supported by the KSX II.

Supported Smart Card Readers

Type	Vendor	Model	Verified
USB	SCM Microsystems	SCR331	Verified on local and remote
USB	ActivIdentity®	ActivIdentity USB Reader v2.0	Verified on local and remote
USB	ActivIdentity	ActivIdentity USB Reader v3.0	Verified on local and remote
USB	Gemalto®	GemPC USB-SW	Verified on local and remote
USB Keyboard/Card reader Combo	Dell®	USB Smart Card Reader Keyboard	Verified on local and remote
USB Keyboard/Card reader Combo	Cherry GmbH	G83-6744 SmartBoard	Verified on local and remote
USB reader for SIM-sized cards	Omnikey	6121	Verified on local and remote
Integrated (Dell Latitude D620)	O2Micro	OZ776	Remote only
PCMCIA	ActivIdentity	ActivIdentity PCMCIA Reader	Remote only
PCMCIA	SCM Microsystems	SCR243	Remote only

Note: SCM Microsystems SCR331 smart card readers must be using SCM Microsystems firmware v5.25.

Unsupported Smart Card Readers

This table contains a list of readers that Raritan has tested with the KSX II and we know not to work, therefore they are unsupported. If a smart card reader does not appear in the supported smart card readers table or in the unsupported smart card readers table, Raritan cannot guarantee it will function with the KSX II.

Type	Vendor	Model	Notes
USB Keyboard/Card reader Combo	HP®	ED707A	No interrupt endpoint => not compatible with Microsoft® driver
USB Keyboard/Card reader Combo	SCM Microsystems	SCR338	Proprietary card reader implementation (not CCID-compliant)
USB Token	Aladdin®	eToken PRO™	Proprietary implementation

Minimum System Requirements

Local Port Requirements

The basic interoperability requirement for local port attachment to the KSX II is:

- All devices (smart card reader or token) that are locally attached must be USB CCID-compliant.

Target Server Requirements

When using smart card readers, the basic requirements for interoperability at the target server are:

- The IFD (smart card reader) Handler must be a standard USB CCID device driver (comparable to the generic Microsoft® USB CCID driver).
- A D2CIM-DVUSB (Dual-VM CIM) is required and must be using firmware version 3A6E or later.
- Blade chassis server connections, where a CIM per blade is used, are supported.
- Blade chassis server connections, where a CIM per chassis is used, is only supported for IBM® BladeCenter® models H and E with auto-discovery enabled.

Windows XP Targets

Windows XP® operating system targets must be running Windows XP SP3 in order to use smart cards with the KSX II. If you are working with .NET 3.5 in a Windows XP environment on the target server, you must be using SP1.

Linux Targets

If you are using a Linux® target, the following requirements must be met to use smart card readers with the KSX II.

- CCID Requirements

  If the Raritan D2CIM-DVUSB VM/CCID is not recognized as a smart card reader by your Linux target, you may need to update the CCID driver version to 1.3.8 or above and update the driver configuration file (Info.plist).

Operating system	CCID requirements
RHEL 5	ccid-1.3.8-1.el5
SuSE 11	pcsc-ccid-1.3.8-3.12
Fedora® Core 10	ccid-1.3.8-1.fc10.i386

Remote Client Requirements

The basic requirements for interoperability at the remote client are:

- The IFD (smart card reader) Handler must be a PC/SC compliant device driver.
- The ICC (smart card) Resource Manager must be available and be PC/SC compliant.
- The JRE™ 1.6.x with smart card API must be available for use by the Raritan client application.

Linux Clients

If you are using a Linux® client, the following requirements must be met to use smart card readers with the KSX II.

Note: User login to client, on smart card insertion, may take longer when 1 or more KVM sessions are actively in place to targets.   As the login process to these targets is also under way.

- PC/SC Requirements

Operating system	Required PC/SC
RHEL 5	pcsc-lite-1.4.4-0.1.el5

SuSE 11	pcsc-lite-1.4.102-1.24
Fedora® Core 10	pcsc-lite-1.4.102.3.fc10.i386

- Create a Java™ Library Link

  A soft link must be created to the libpcsclite.so after upgrading RHEL 4, RHEL 5 and FC 10. For example, ln –s /usr/lib/libpcsclite.so.1 /usr/lib/libpcsclite.so, assuming installing the package places the libraries in /usr/lib or /user/local/lib.

- PC/SC Daemon

  When the pcsc daemon (resource manager in framework) is restarted, restart the browser and MPC, too.

Environmental Requirements

Operating	
Temperature	0°C- 40°C (32°F - 104°F)
Humidity	20% - 85% RH
Altitude	N/A
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A
Non-Operating	
Temperature	0°C- 50°C (32°F - 122°F)
Humidity	10% - 90% RH
Altitude	N/A
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A

Emergency Connectivity

Connection	Description
Optional modem connectivity	For emergency remote access if the network has failed.
Target device connectivity	Simplified RJ45-based CAT 5 cable scheme; serial port adapters are available from Raritan.

Local access	Local Access for "crash-cart" applications.

See ***Connectivity*** (on page 290) for a list of necessary KSX II hardware (adapters and/or cables) for connecting the KSX II to common Vendor/Model combinations.

Electrical Specifications

Parameter	Value
Input	
Nominal Frequencies	50/60 Hz
Nominal Voltage Range	100/240 VAC
Maximum Current AC RMS	0.6A max.
AC Operating Range	100 to 240 VAC (+-10%), 47 to 63 Hz

Remote Connection

Remote connection	Details
Network	10BASE-T, 100BASE-T, and 1000BASE-T (Gigabit) Ethernet
Protocols	TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP/LDAPS

KVM Properties

- Keyboard - PS/2 or USB
- Mouse - PS/2 or USB
- Video - VGA

Ports Used

Port	Description
HTTP, Port 80	All requests received by KSX II via HTTP (port 80) are automatically forwarded to HTTPS for complete security. The KSX II responds to Port 80 for user convenience, relieving users from having to explicitly type "https://" in the URL

Port	Description
	field to access the KSX II, but while still preserving complete security.
HTTPS, Port 443	This port is used for the actual KVM-over-IP communication from the KSX II device to the KVM client on the user's desktop. It cannot be changed.
KSX II (Raritan KVM-over-IP) Protocol, Configurable Port 5000	This port is used to discover other KX devices and for communication between Raritan devices and systems, including CC-SG and MPC. By default, this is set to Port 5000, but you may configure it to use any TCP port of your choice (except 80 and 443). For details on how to configure this setting, refer to *Network Settings* (on page 135).
SNTP (Time Server) on Configurable UDP Port 123 **Optional**	The KSX II offers the optional capability to synchronize its internal clock to a central time server. This function requires the use of UDP Port 123 (the standard for SNTP), but can also be configured to use any port of your designation.
LDAP/LDAPS on Configurable Ports 389 and 636 **Optional**	If the KSX II is configured to remotely authenticate user logins via the LDAP/LDAPS protocol, ports 389 and 636 will be used, but the system can also be configured to use any port of your designation.
RADIUS on Configurable Port 1812 **Optional**	If the KSX II is configured to remotely authenticate user logins via the RADIUS protocol, either port 1812 or 1813 will be used, but the system can also be configured to use any port of your designation.
RADIUS Accounting on Configurable Port 1813	If the KSX II is configured to remotely authenticate user logins via the RADIUS protocol, and also employs RADIUS accounting for event logging, port 1813 or an additional port of your designation will be used to transfer log notifications.
SYSLOG on Configurable UDP Port 514	If the KSX II is configured to send messages to a Syslog server, then the indicated port(s) will be used for communication - uses UDP Port 514.
SNMP Default UDP Ports **Optional**	Port 161 is used for inbound/outbound read/write SNMP access and port 162 is used for outbound traffic for SNMP traps.
SSH	(Secure Shell) SSH port can be configured.

Port	Description
	The default is port 22.
Telnet	Telnet port can be configured but is not recommended. The default port is 23.

Target Server Connection Distance and Video Resolution

The maximum supported distance is a function of many factors including the type/quality of Cat5 cable, server type and manufacturer, video driver and monitor, environmental conditions, and user expectations. The following table summarizes the maximum target server distance for various video resolutions and refresh rates:

Video resolution	Refresh rate	Maximum distance
1600x1200	60	50 ft. (15 m)
1280x1024	60	100 ft. (30 m)
1024x768	60	150 ft. (45 m)

Note: Due to the multiplicity of server manufacturers and types, OS versions, video drivers, and so forth and the subjective nature of video quality, Raritan cannot guarantee performance across all distances in all environments.

See the **Supported Video Resolutions** (on page 279) for the video resolutions supported by the KSX II.

Distances for Serial Devices

Following are the standard distances for serial devices:
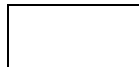
Baud rate-feet
2400 - 400 ft.
4800 - 200 ft.
9600 - 100 ft.
19200 - 50 ft.
38400 - 25 ft.
57600 - 16 ft.
115200 - 8 ft.

Network Speed Settings

KSX II network speed setting						
Network switch port setting	**Auto**	**1000/Full**	**100/Full**	**100/Half**	**10/Full**	**10/Half**
Auto	Highest Available Speed	1000/Full	KSX II: 100/Full Switch: 100/Half	100/Half	KSX II: 10/Full Switch: 10/Half	10/Half
1000/Full	1000/Full	1000/Full	No Communication	No Communication	No Communication	No Communication
100/Full	KSX II: 100/Half Switch: 100/Full	KSX II: 100/Half Switch: 100/Full	100/Full	KSX II: 100/Half Switch: 100/Full	No Communication	No Communication
100/Half	100/Half	100/Half	KSX II: 100/Full Switch: 100/Half	100/Half	No Communication	No Communication
10/Full	KSX II: 10/Half Switch: 10/Full	No Communication	No Communication	No Communication	10/Full	KSX II: 10/Half Switch: 10/Full
10/Half	10/Half	No Communication	No Communication	No Communication	KSX II: 10/Full Switch: 10/Half	10/Half
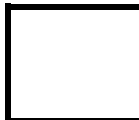
Legend:

Does not function as expected

Supported

   	Functions; not recommended
   	NOT supported by Ethernet specification; product will communicate, but collisions will occur
	Per Ethernet specification, these should be "no communication," however, note that the KSX II behavior deviates from expected behavior

Note: For reliable network communication, configure the KSX II and the LAN switch to the same LAN Interface Speed and Duplex. For example, configure both the KSX II and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100MB/s/Full.

Connectivity

The following table lists the necessary KSX II hardware (adapters and/or cables) for connecting the KSX II to common vendor/model combinations.

Vendor	Device	Console connector	Serial connection
Checkpoint	Firewall	DB9M	ASCSDB9F adapter and a CAT 5 cable
Cisco	PIX Firewall		
Cisco	Catalyst	RJ-45	CRLVR-15 rollover cable; or CRLVR-1 adapter cable and a CAT5 cable CRLVR-1 cable for connecting a terminal port (RJ-45 Connector type) of KSX II-48 models that have this connector to another KSX II.
Cisco	Router	DB25F	ASCSDB25M adapter and a CAT 5 cable
Hewlett Packard®	UNIX® Server	DB9M	ASCSDB9F adapter and a

Vendor	Device	Console connector	Serial connection
Silicon Graphics	Origin		CAT 5 cable
Sun™	SPARCStation	DB25F	ASCSDB25M adapter and a CAT 5 cable
Sun	Netra T1	RJ-45	CRLVR-15 cable; or CRLVR-1 adapter and a CAT5 cable
Sun	Cobalt	DB9M	ASCSDB9F adapter and a CAT 5 cable
Various	Windows NT®		

Go to the Support page on Raritan's website (www.raritan.com) to obtain a list of commonly used cables and adapters.

KSX II Serial RJ-45 Pinouts

To provide maximum port density and to enable simple UTP (Category 5) cabling, The KSX II provides its serial connections via compact RJ-45 ports. However, no widely adopted industry-standard exists for sending serial data over RJ-45 connections.

The following tables list the RJ-45 pinouts for the RJ-45 connector.

RJ-45 PIN	SIGNAL
1	RTS
2	DTR
3	TxD
4	GND
5	DCD
6	RxD
7	DSR
8	CTS

Go to the Raritan website (www.raritan.com) Support page to find the latest information about the KSX II serial pinouts (RJ-45).

DB9F Nulling Serial Adapter Pinouts

291

RJ-45 (female)	DB9 (female)
1	8
2	1, 6
3	2
4	SHELL
5	5
6	3
7	4
8	7

DB9M Nulling Serial Adapter Pinouts

RJ-45 (female)	DB9 (male)
1	8
2	1, 6
3	2
4	SHELL
5	5
6	3
7	4
8	7

DB25F Nulling Serial Adapter Pinouts

RJ-45 (female)	DB25 (female)
1	5
2	6, 8
3	3
4	1
5	7
6	2
7	20

RJ-45 (female)	DB25 (female)
8	4

DB25M Nulling Serial Adapter Pinouts

RJ-45 (female)	DB25 (male)
1	5
2	6, 8
3	3
4	1
5	7
6	2
7	20
8	4

Appendix B Updating the LDAP/LDAPS Schema

IMPORTANT: The procedures in this chapter should be attempted only by experienced users.

In This Chapter

Returning User Group Information

Use the information in this section to return User Group information (and assist with authorization) once authentication is successful.

From LDAP/LDAPS

When an LDAP/LDAPS authentication is successful, the KSX II determines the permissions for a given user based on the permissions of the user's group. Your remote LDAP server can provide these user group names by returning an attribute named as follows:

rciusergroup   attribute type: string

This may require a schema extension on your LDAP/LDAPS server. Consult your authentication server administrator to enable this attribute.

In addition, for Microsoft® Active Directory®, the standard LDAP memberOf is used.

From Microsoft Active Directory

Note: This should be attempted only by an experienced Active Directory® administrator.

Returning user group information from Microsoft's® Active Directory for Windows 2000® operating system server requires updating the LDAP/LDAPS schema. See your Microsoft documentation for details.

1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.

2. Run Active Directory Console and select Active Directory Schema.

Setting the Registry to Permit Write Operations to the Schema

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

► **To permit write operations to the schema:**

1. Right-click the Active Directory® Schema root node in the left pane of the window and then click Operations Master. The Change Schema Master dialog appears.
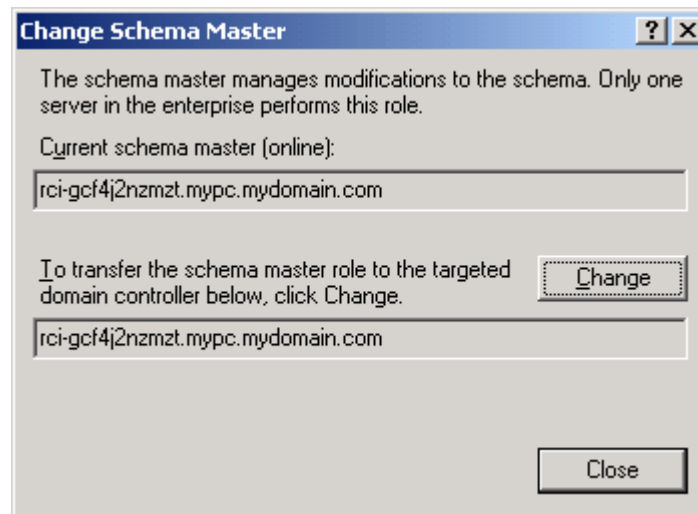
2. Select the "Schema can be modified on this Domain Controller" checkbox. **Optional**

3. Click OK.

Creating a New Attribute

► **To create new attributes for the rciusergroup class:**

1. Click the + symbol before Active Directory® Schema in the left pane of the window.

2. Right-click Attributes in the left pane.

3. Click New and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute dialog appears.

4. Type *rciusergroup* in the Common Name field.

5. Type *rciusergroup* in the LDAP Display Name field.

6. Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.

7. Type a meaningful description in the Description field.

8. Click the Syntax drop-down arrow and choose Case Insensitive String from the list.

9. Type *1* in the Minimum field.

10. Type *24* in the Maximum field.

11. Click OK to create the new attribute.

Adding Attributes to the Class

▶ **To add attributes to the class:**

1. Click Classes in the left pane of the window.

2. Scroll to the user class in the right pane and right-click it.
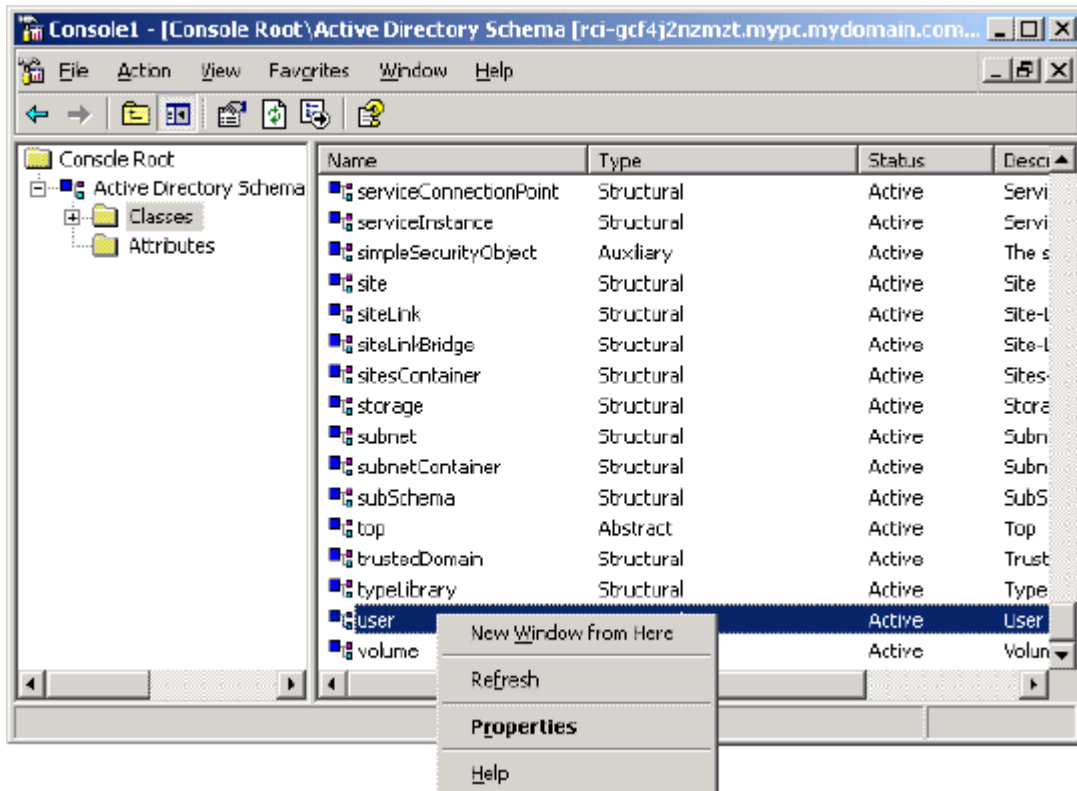
3. Choose Properties from the menu. The user Properties dialog appears.

4. Click the Attributes tab to open it.

5. Click Add.

6. Choose rciusergroup from the Select Schema Object list.
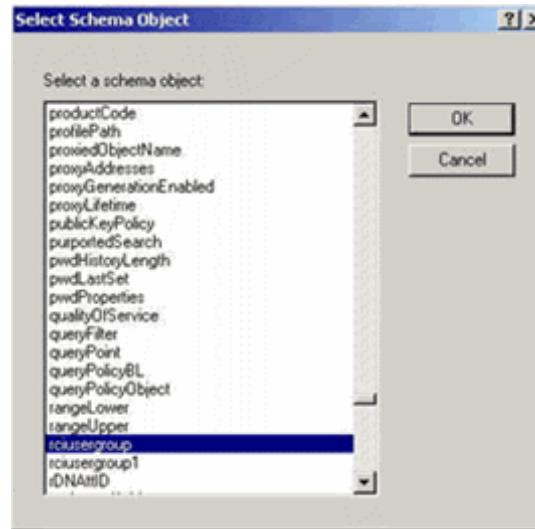
7. Click OK in the Select Schema Object dialog.

8. Click OK in the User Properties dialog.

Updating the Schema Cache

► **To update the schema cache:**

1. Right-click Active Directory® Schema in the left pane of the window and select Reload the Schema.

2. Minimize the Active Directory Schema MMC (Microsoft® Management Console) console.

Editing rciusergroup Attributes for User Members

To run the Active Directory® script on a Windows 2003® server, use the script provided by Microsoft® (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft® Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service.

► **To edit the individual user attributes within the group rciusergroup:**

1. From the installation CD, choose Support > Tools.

2. Double-click SUPTOOLS.MSI to install the support tools.

3. Go to the directory where the support tools were installed. Run adsiedit.msc. The ADSI Edit window opens.
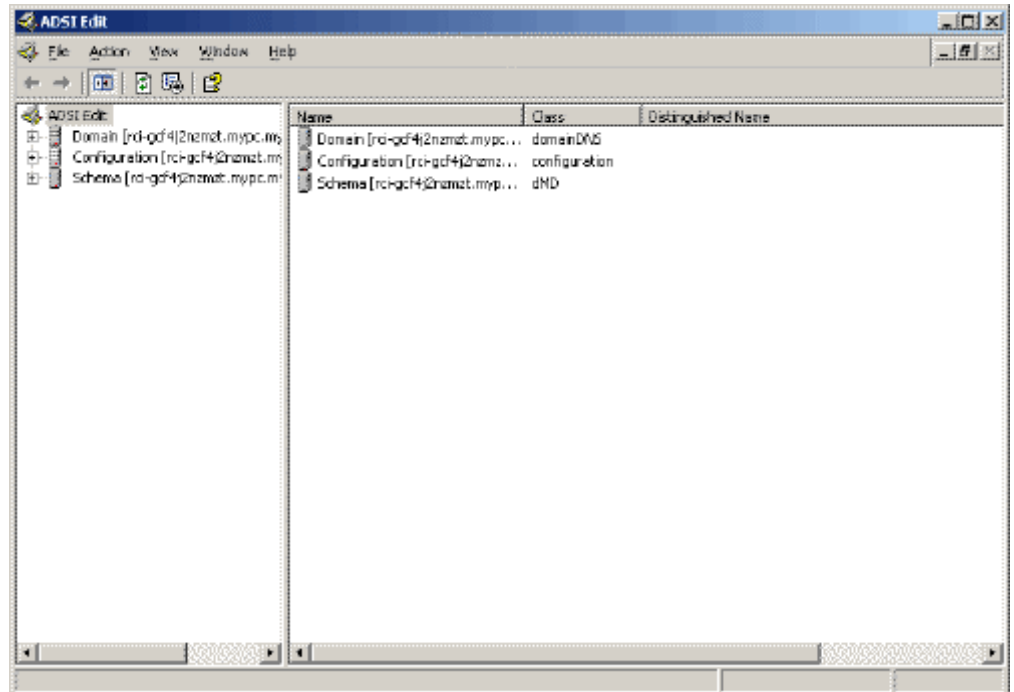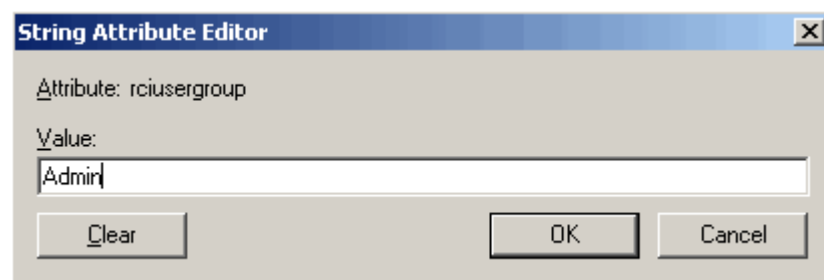

4. Open the Domain.

5. In the left pane of the window, select the CN=Users folder.
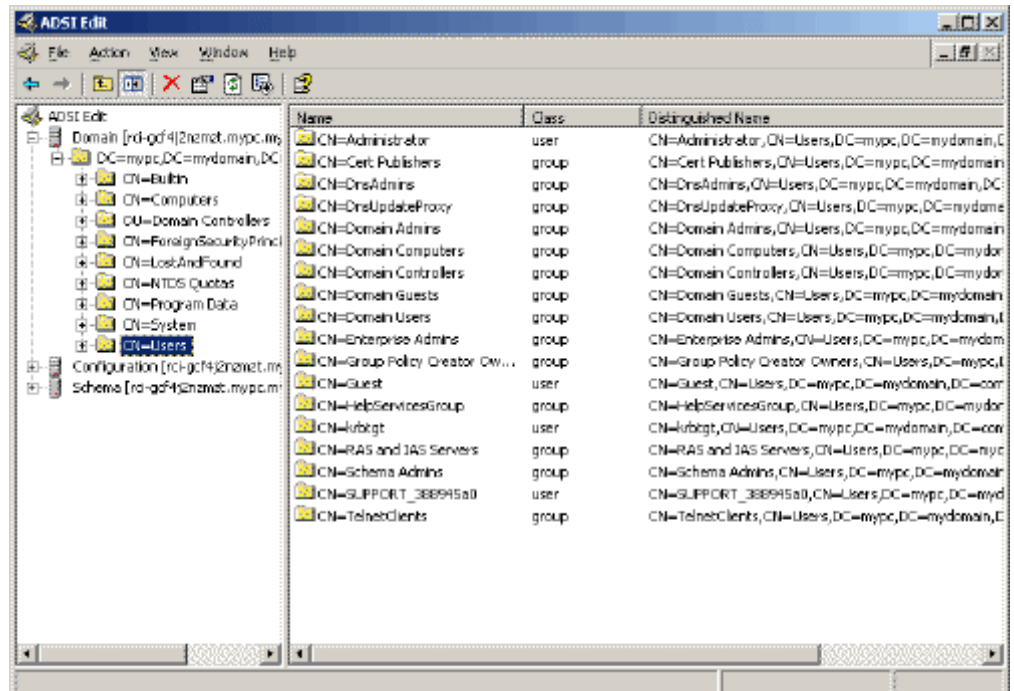
6. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.

7. Click the Attribute Editor tab if it is not already open. Choose rciusergroup from the Attributes list.
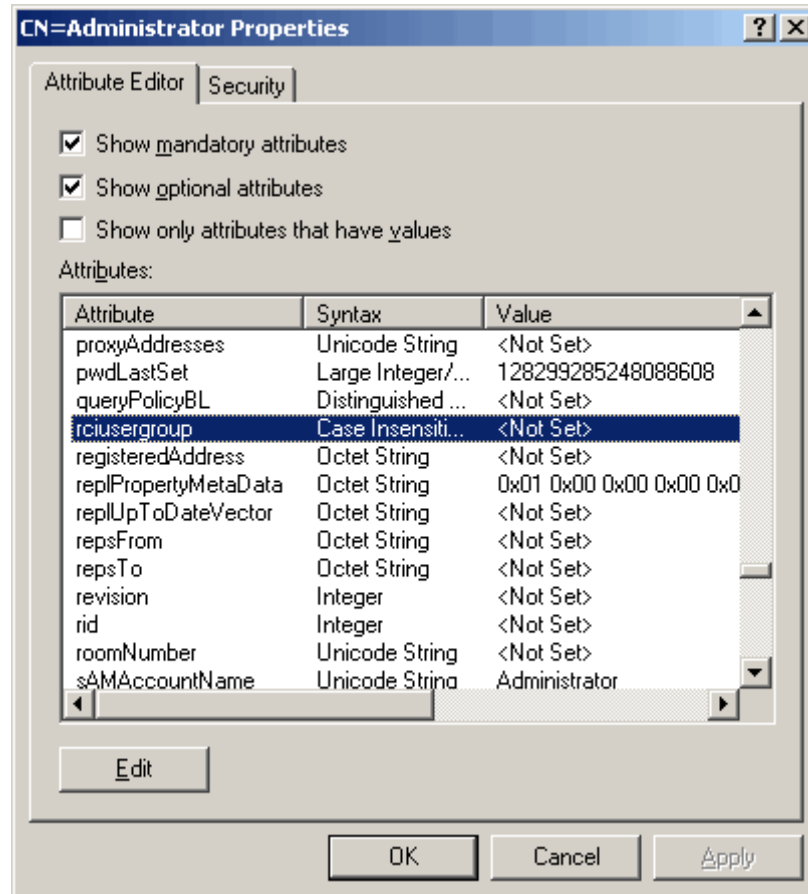
8. Click Edit. The String Attribute Editor dialog appears.

9. Type the user group (created in the KSX II) in the Edit Attribute field. Click OK.

Appendix C Informational Notes

In This Chapter

Overview

This section includes important notes on KSX II usage. Future updates will be documented and available online through the Help link in the KSX II Remote Console interface.

Java

AES 256 Prerequisites and Supported Configurations for Java

Applications	Prerequisites	Supported
Standalone MPC	Requires installation of Java Cryptography Extension® (JCE®) Unlimited Strength Jurisdiction Policy Files +	Yes
Standalone RSC	Requires installation of Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files +	Yes

Applications	Prerequisites	Supported	
MPC Applet	Requires installation of Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files +	**Browser**	**Supported**
		Firefox® 2.0.0.7	Yes
		Firefox 3.0.x	Yes
		Internet Explorer® 6*	No
		Internet Explorer 7	Yes
		Internet Explorer 8	Yes
HTML access client	Requires installation of Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files +	**Browser**	**Supported**
		Firefox 2.0.0.7	Yes
		Firefox 3.0.x	Yes
		Internet Explorer 6 *	No
		Internet Explorer 7	Yes
		Internet Explorer 8	Yes

+ Jurisdiction files for various JREs™ are available in the Other Downloads on the Java™ Sun™ site.

JRE	Link
JRE1.6	http://java.sun.com/javase/downloads/index.jsp

* In addition, IE6 does not support AES 128.

Java Runtime Environment (JRE)

Important: It is recommended that you disable Java™ caching and clear the Java cache. Please refer to your Java documentation for more information.

The KSX II Remote Console and MPC require JRE™ to function. Java Runtime Environment™ (JRE) version 1.6.x or higher are supported. The KSX II Remote Console checks the Java version. If the version is incorrect or outdated, you will be prompted to download a compatible version.

Note: In order for multi-language keyboards to work in the KSX II Remote Console (Virtual KVM Client), install the multi-language version of Java Runtime Environment (JRE).

IPv6 Support Notes

Java

Java™ 1.6 supports IPv6 for the following:

- Solaris™ 8 and higher

- Linux® kernel 2.1.2 and higher (RedHat 6.1 and higher)

Java 5.0 and above supports the IPv6 for the following:

- Solaris 8 and higher

- Linux kernel 2.1.2 and higher (kernel 2.4.0 and higher recommended for better IPv6 support)

- Windows XP® SP1 and Windows 2003®, Windows Vista® operating systems

The following IPv6 configurations *are not* supported by Java:

- J2SE 1.4 does not support IPv6 on Microsoft® Windows®.

Linux

- It is recommended that Linux kernel 2.4.0 or higher is used when using IPv6.

- An IPv6-enabled kernel will need to be installed or the kernel will need to be rebuilt with IPv6 options enabled.

- Several network utilities will also need to be installed for Linux when using IPv6. For detailed information, refer to http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html

Windows

- Windows XP and Windows 2003 users will need to install the Microsoft IPV6 service pack to enable IPV6.

Mac Leopard

- IPv6 is not supported in KSX II version 2.0.20 for Mac® Leopard®.

Samba

- IPv6 is not supported for use with virtual media when using Samba.

Keyboards

Non-US Keyboards

French Keyboard

Caret Symbol (Linux® Clients Only)

The Virtual KVM Client and the Multi-Platform Client (MPC) do not process the key combination of Alt Gr + 9 as the caret symbol (^) when using French keyboards with Linux clients.

▶ **To obtain the caret symbol:**

From a French keyboard, press the ^ key (to the right of the P key), then immediately press the space bar.

Alternatively, create a macro consisting of the following commands:

1. Press Right Alt
2. Press 9.
3. Release 9.
4. Release Right Alt.

Note: These procedures do not apply to the circumflex accent (above vowels). In all cases, the ^ key (to the right of the P key) works on French keyboards to create the circumflex accent when used in combination with another character.

Accent Symbol (Windows XP® Operating System Clients Only)

From the Virtual KVM Client and the Multi-Platform Client, the key combination of Alt Gr + 7 results in the accented character displaying twice when using French keyboards with Windows XP clients.

Note: This does not occur with Linux clients.

Numeric Keypad

From the Virtual KVM Client and the Multi-Platform Client, the numeric keypad symbols display as follows when using a French keyboard:

Numeric keypad symbol	Displays as
/	;
.	;

Tilde Symbol

From the Virtual KVM Client and the Multi-Platform Client, the key combination of Alt Gr + 2 does not produce the tilde (~) symbol when using a French keyboard.

▶ **To obtain the tilde symbol:**

Create a macro consisting of the following commands:

- Press right Alt.
- Press 2.
- Release 2.
- Release right Alt.

Keyboard Language Preference (Fedora Linux Clients)

Because the Sun™ JRE™ on Linux® has problems generating the correct KeyEvents for foreign-language keyboards configured using System Preferences, Raritan recommends that you configure foreign keyboards using the methods described in the following table.

Language	Configuration method
US Intl	Default
UK	System Settings (Control Center)
French	Keyboard Indicator
German	Keyboard Indicator
Hungarian	System Settings (Control Center)
Spanish	System Settings (Control Center)
Swiss-German	System Settings (Control Center)
Norwegian	Keyboard Indicator
Swedish	Keyboard Indicator
Danish	Keyboard Indicator
Japanese	System Settings (Control Center)
Korean	System Settings (Control Center)
Slovenian	System Settings (Control Center)
Italian	System Settings (Control Center)
Portuguese	System Settings (Control Center)

Note: The Keyboard Indicator should be used on Linux systems using Gnome as a desktop environment.

When using a Hungarian keyboard from a Linux client, the Latin letter U with Double Acute and the Latin letter O with Double Acute work only with JRE 1.6.

There are several methods that can be used to set the keyboard language preference on Fedora® Linux clients. The following method must be used in order for the keys to be mapped correctly from the Virtual KVM Client and the Multi-Platform Client (MPC).

▶ **To set the keyboard language using System Settings:**

1. From the toolbar, choose System > Preferences > Keyboard.

2. Open the Layouts tab.

3. Add or select the appropriate language.

4. Click Close.

▶ **To set the keyboard language using the Keyboard Indicator:**

1. Right-click the Task Bar and choose Add to Panel.

2. In the Add to Panel dialog, right-click the Keyboard Indicator and from the menu choose Open Keyboard Preferences.

3. In the Keyboard Preferences dialog, click the Layouts tab.

4. Add and remove languages as necessary.

Key Combinations and the Java Runtime Environment (JRE)

Because of a limitation in the Java Runtime Environment™ (JRE™), Fedora®, Linux®, and Solaris™ clients receive an invalid response from Alt Gr on UK English and US International language keyboards. Fedora, Linux, and Solaris do not pick up events for the Alt Gr key combination for Java™ 1.5. Java 1.6 appears to improve on this, although the keyPressed and keyReleased events for Alt Gr still identify it as an "unknown key code".

Also, a key pressed in combination with Alt Gr (such as on the UK keyboard Alt Gr-4, which is the Euro symbol), will only generate a keyTyped followed by a keyReleased event for that value without a keyPressed event. Java 1.6 improves upon this by filling in the keyPressed event as well.

Macintosh Keyboard

When a Macintosh® is used as the client, the following keys on the Mac® keyboard are not captured by the Java™ Runtime Environment (JRE™):

- F9
- F10
- F11
- F14
- F15
- Volume Up
- Volume Down
- Mute
- Eject

As a result, the Virtual KVM Client and the Multi-Platform Client (MPC) are unable to process these keys from a Mac client's keyboard.

Dell Chassis Cable Lengths and Video Resolutions

In order to maintain video quality, Raritan recommends using the following cable lengths and video resolutions when you are connecting to Dell® blade chassis from the KSX II:

Cable length	Video resolution
50 ft.	1024x768x60
50 ft.	1280x1024x60
30 ft.	1600x1200x60

Fedora

Resolving Fedora Core Focus

Using the Multi-Platform Client (MPC), occasionally there is an inability to log in to a KSX II device or to access KVM target servers (Windows®, SUSE, and so forth). In addition, the Ctrl+Alt+M key combination may not bring up the Keyboard Shortcut menu. This situation occurs with the following client configuration: Fedora® Core 6 and Firefox® 1.5 or 2.0.

Through testing, it has been determined that installation of libXp resolves window focusing issues with Fedora Core 6. Raritan has tested with libXp-1.0.0.8.i386.rpm; this resolved all of the keyboard focus and popup-menu problems.

Note: libXp is also required for the SeaMonkey (formerly Mozilla®) browser to work with the Java™ plug-in.

Mouse Pointer Synchronization (Fedora)

When connected in dual mouse mode to a target server running Fedora® 7, If the target and local mouse pointers lose synchronization, changing the mouse mode from or to Intelligent or Standard may improve synchronization. Single mouse mode may also provide for better control.

▶ **To resynchronize the mouse cursors:**

- Use the Synchronize Mouse option from the Virtual KVM Client.

VKC and MPC Smart Card Connections to Fedora Servers

If you are using a smart card to connect to a Fedora® server via MPC or VKC upgrade the pcsc-lite library to 1.4.102-3 or above.

Resolving Issues with Firefox Freezing when Using Fedora

If you are accessing Firefox® and are using a Fedora® server, Firefox may freeze when it is opening. To resolve this issue, install the libnpjp2.so Java™ plug-in on the server.

USB Ports and Profiles

VM-CIMs and DL360 USB Ports

HP® DL360 servers have one USB port on the back of the device and another on the front of the device. With the DL360, both ports cannot be used at the same time. Therefore, a dual VM-CIM cannot be used on DL360 servers.

However, as a workaround, a USB2 hub can be attached to the USB port on the back of the device and a dual VM-CIM can be attached to the hub.

Help for Choosing USB Profiles

When you are connected to a KVM target server in VKC, you can view information about USB profiles via the Help on USB Profiles command on the USB Profile menu.
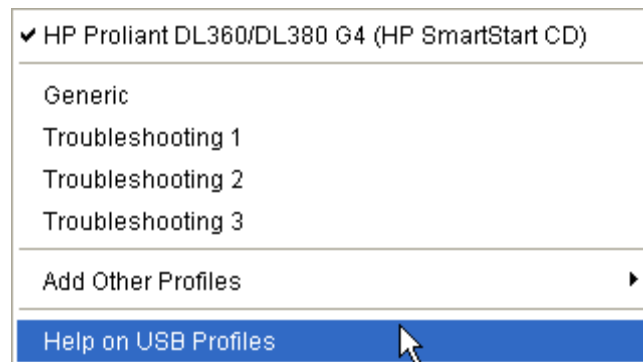
USB profile help appears in the USB Profile Help window. For detailed information about specific USB profiles, see ***Available USB Profiles*** (on page 105).

Raritan provides a standard selection of USB configuration profiles for a wide range of operating system and BIOS level server implementations. These are intended to provide an optimal match between remote USB device and target server configurations.

The 'Generic' profile meets the needs of most commonly deployed target server configurations.

Additional profiles are made available to meet the specific needs of other commonly deployed server configurations (for example, Linux®, MAC OS-X®).

There are also a number of profiles (designated by platform name and BIOS revision) that have been tailored to enhance the   virtual media function compatibility with the target server, for example, when operating at the BIOS level.

'Add Other Profiles' provides access to other profiles available on the system. Profiles selected from this list will be added to the USB Profile Menu. This includes a set of 'trouble-shooting' profiles intended to help identify configuration limitations.

The USB Profile Menu selections are configurable via the Console Device Settings > Port Configuration page.

Should none of the standard USB profiles provided by Raritan meet your target server requirements, Raritan Technical Support can work with you to arrive at a solution tailored for that target. Raritan recommends that you do the following:

1. Check the most recent release notes on the Raritan website (www.raritan.com) on the Firmware Upgrade page to see if a solution is already available for your configuration.

2. If not, please provide the following information when contacting Raritan Technical Support:

    a. Target server information, manufacturer, model, BIOS, manufacturer, and version.

    b. The intended use (e.g. redirecting an image to reload a server's operating system from CD).

Changing a USB Profile when Using a Smart Card Reader

There may be certain circumstances under which you will need to change the USB profile for a target server. For example, you may need to change the connection speed to "Use Full Speed for Virtual Media CIM" when the target has problems with the "High Speed USB" connection speed.

When a profile is changed, you may receive a New Hardware Detected message and be required to log in to the target with administrative privileges to reinstall the USB driver. This is only likely to occur the first few times the target sees the new settings for the USB device. Afterward, the target will select the driver correctly.

SUSE/VESA Video Modes

The SuSE X.org configuration tool SaX2 generates video modes using modeline entries in the X.org configuration file. These video modes do not correspond exactly with VESA video mode timing (even when a VESA monitor is selected). The KSX II, on the other hand, relies on exact VESA mode timing for proper synchronization. This disparity can result in black borders, missing sections of the picture, and noise.

▶ **To configure the SUSE video display:**

1. The generated configuration file /etc/X11/xorg.conf includes a Monitor section with an option named UseModes. For example, UseModes "Modes[0]"

2. Either comment out this line (using #) or delete it completely.

3. Restart the X server.

With this change, the internal video mode timing from the X server will be used and will correspond exactly with the VESA video mode timing, resulting in the proper video display on the KSX II.

CIMs

Windows 3-Button Mouse on Linux Targets

When using a 3-button mouse on a Windows® client connecting to a Linux® target, the left mouse button may get mapped to the center button of the Windows client 3-button mouse.

311

Virtual Media

Dell OptiPlex and Dimension Computers

From certain Dell OptiPlex ™ and Dimension computers, it may not be possible to boot a target server from a redirected drive/ISO image, or to access the target server BIOS when a virtual media session is active (unless the Use Full Speed for Virtual Media CIM option is enabled from the Port page).

Note: ISO9660 format is the standard supported by Raritan. However, other CD-ROM extensions may also work.

Accessing Virtual Media on a Windows 2000 Server Using a D2CIM-VUSB

A virtual media local drive cannot be accessed   on a Windows 2000® server using a D2CIM-VUSB.

Virtual Media Not Refreshed After Files Added

After a virtual media drive has been mounted, if you add a file(s) to that drive, those files may not be immediately visible on the target server. Disconnect and then reconnect the virtual media connection.

Target BIOS Boot Time with Virtual Media

The BIOS for certain targets may take longer to boot if media is mounted virtually at the target.

▶ To shorten the boot time:

1. Close the Virtual KVM Client to completely release the virtual media drives.

2. Restart the target.

Virtual Media Connection Failures Using High Speed for Virtual Media Connections

Under certain circumstances it may be necessary to select the "Use Full Speed for Virtual Media CIM" when a target has problems with "High Speed USB" connections or when the target is experiencing USB protocol errors caused by signal degradation due to additional connectors and cables (for example, a connection to a blade server via a dongle).

CC-SG

Virtual KVM Client Version Not Known from CC-SG Proxy Mode

When the Virtual KVM Client is launched from CommandCenter Secure Gateway (CC-SG) in proxy mode, the Virtual KVM Client version is unknown. In the About Raritan Virtual KVM Client dialog, the version is displayed as "Version Unknown".

Single Mouse Mode - Connecting to a KSX II Target Under CC-SG Control Via VKC Using Firefox

When using Firefox® to connect to a KSX II target under CC-SG control using DCIM-PS2 or DCIM-USBG2, if you change to Single Mouse Mode in the Virtual KVM Client, the VKC window will no longer be the focus window and the mouse will not respond. If this occurs, left click on the mouse or press Alt+Tab to return the focus to the VKC window.

Moving Between Ports of the KSX II

If you move a between ports of the same KSX II and resume management within one minute, CC-SG may display an error message. If you resume management, the display will be updated.

Appendix D   FAQs

In This Chapter

General Questions

What is KSX II?

The KSX II is a second generation digital KVM (Keyboard, Video Mouse) switch that enables IT administrators to access and control 8, 16, 32, or 64* servers over the network with BIOS-level functionality. The KSX II is completely hardware and OS-independent; users can troubleshoot and reconfigure servers even when servers are down.

At the rack, the KSX II provides the same functionality, convenience, space savings, and cost savings as traditional analog KVM switches. However, the KSX II also integrates the industry's highest-performing KVM-over-IP technology, allowing multiple administrators to access server KVM consoles from any networked workstation.

The KSX II is completely hardware and OS-independent; users can troubleshoot and reconfigure servers even when servers are down.

How does the KSX II differ from remote control software?

When using the KSX II remotely, the interface, at first glance, may seem similar to remote control software such as pcAnywhere™, Windows Terminal Services/Remote Desktop®, VNC, and so forth. However, because the KSX II is not a software but a hardware solution, it's much more powerful. Specifically:

- OS- and hardware-independent - The KSX II can be used to manage servers running many popular operating systems, including Intel®, Sun™, PowerPC running Windows®, Linux®, Solaris™, etc.

- State-Independent/Agentless - The KSX II does not require the managed server's operating system to be up and running, nor does it require any special software to be installed on the managed server.

- Out-of-Band - Even if the managed server's own network connection is unavailable, it can still be managed through the KSX II.

- BIOS-Level Access - Even if the server is hung at boot up, requires booting to safe mode or requires system BIOS parameters to be altered, the KSX II still works flawlessly to enable these configurations to be made.

- OS- and hardware-independent - KSX II can be used to manage servers running many popular operating systems, including Intel, Sun, PowerPC running Windows, Linux, Solaris, and so forth.

How do the new features of the KSX II compare to the KSX I?

The KSX II has many new and exciting features, including virtual media, dual gigabit Ethernet, next generation local port, enhanced support for serial ports, and so forth.

How do I migrate from the Dominion KSX I to the KSX II?

In general, customers can continue to use their existing switches for many years. As their data centers expand, customers can purchase and use the new KSX II models. Raritan's centralized management unit, CommandCenter Secure Gateway, and the Multi-Platform Client (MPC) both support KSX I and KSX II switches seamlessly.

What CIMs are supported for the KSX II switch?

Refer to *Supported Operating Systems and CIMs (KVM Target Servers)* (on page 271).

Can the KSX II be rack mounted?

Yes. The KSX II ships standard with 19" rack mount brackets. It can also be reverse rack mounted so the server ports face forward.

How large is the KSX II?

The KSX II is only 1U high, fits in a standard 19" rack mount, and is only 11.4" (29 cm) deep.

Serial Access

My Dominion KSX II has just been configured with a network address and I can successfully ping the IP, but when I try to access it using a web browser, the message reads "Page cannot be found or server error, contact System Administrator."

Check your web browser settings and confirm that a proxy server is being used. If so, click the "Bypass local addresses or configure KSX IP in the exception list" checkbox. Next, make sure the web browser has 128-bit cipher strength. From the Help menu, click About to find this information.

When I select the "Send Break" option from the Emulator menu in Raritan Console (on my KSX II), it does not send a break to my Sun™ server. What could be wrong and how can I address it?

If the SUN machine does not respond to the break signal, verify that the line 'KEYBOARD_ABORT=disable' is commented out in the /etc/default/kbd file (on the Sun machine). If this line is not commented out, it will disable a keyboard abort sequence; comment out this line to enable the sequence.

How can I consolidate the sites where I have a Dominion KSX II installed?

Raritan's CommandCenter is designed specifically to provide centralized management. It is the ideal solution if you are looking to consolidate management of devices such as Dominion KSX II and other Raritan network-based products.

Is the Ethernet port on the KSX II device 10/100/1000 Mbps auto sensing?

The KSX II supports two 10/100/1000 speed Ethernet interfaces, with configurable speed and duplex settings (either auto-detected or manually set).

Does Dominion KSX II support RS422 and RS485?

No. Currently Dominion KSX II supports only asynchronous RS232 (also commonly called serial, even though serial is a broad term that covers more than RS232). RS 422 and RS485 are used in industrial automation and other markets. Dominion KSX II is currently designed for connection to serially managed servers and other devices typically found in the data-center and server rooms. This includes serially controlled power strips like Raritan's line of remote power control devices.

I have a server/serially managed device that is more than 300 feet from the KSX II - how do I connect?

You will need to purchase a 3rd party RS232 to RS422/485 converter for each end (two units total) - one at the Dominion end and one connected to the device.

Can I open multiple windows and "tile" to monitor multiple servers and other IT equipment?

Yes, you may monitor and "tile" as many windows as there are serial ports on the Dominion KSX II.

I manage many servers. How do I select a server to connect to?

From a browser, a simple menu provides the user-assigned name of each server. Users simply click a server to open a pop-up menu and select Connect from the menu in order to connect to its console port. When using SSH/telnet, the user gets a list of ports they are authorized to connect with when they log on.

As a user, do I see all servers connected to a Dominion KSX II?

No. Each user sees only a list of servers they are authorized to manage/view. The administrator of the Dominion KSX II sets up the access privileges to each server.

Does Dominion KSX II work with Raritan's CommandCenter™?

Yes, Dominion KSX II is deployable as part of an enterprise-wide management solution with Raritan's CommandCenter™. Hundreds of Dominion KSX II units can be managed via CommandCenter.

Is the modem used only for administering the Dominion KSX II itself?

No. Unlike other products in its category, Dominion KSX II offers modem access to administer the box AND get to the target servers.

Is a modem standard on any Dominion KSX II models?

Yes, a built-in modem is standard on KSX II models.

What level of control does Dominion KSX II have over attached target servers?

The remote user has direct command line access and total control of target devices for maintenance, administration, troubleshooting, and even rebooting. User rights are only restricted by their log-in privileges on Dominion KSX II and the server itself.

Why do I need to use a serial adapter to connect to some servers?

While EIA published a standard for RS232 on DB25 and DB9 connectors, there is no standard for RS232 on RJ45. Also, some manufacturers have chosen not to follow the pin out assignments of the EIA on DB25 and DB9 connectors.

Is the Dominion KSX II device SUN® "break-safe"?

All Dominion KSX II units are SUN "break-safe" for use with SUN Solaris.

I have lost my Admin password to the Dominion KSX II. Is there a back door or secret password?

There is no back-door password. The only option is to restore the unit to its factory default settings and create the administrator user name and password again. A hardware reset function to restore the unit to factory default facility is provided.

What remote access connection methods can KSX II accommodate?

Dominion KSX II provides multiple choices for remote access. These include: Internet, LAN/WAN, or dial-up modem. That means servers can be accessed both in and out of band so remote access to mission critical target servers is always available-even if the network is down.

Which ports need to be open on the corporate firewall for a secure console session using Dominion KSX II?

Port 443 (for https), port 5000 Discover and Telnet port 23 (this is optional and does not open by default); optionally port 80 (http) for user sessions. For units running software version 2.2 or higher, port 51000 (or other port between 1024-65536). On software releases PRIOR to firmware 2.2 (2.0Bx or 2.1.x) either port 23 or a user-designated port between 2000 and 2400. When using SSH, port 22 needs to be open.

How do I get access to the operating system of the KSX II?

Dominion KSX II is a secure device. Therefore, NO access is possible to the operating system.

I have a few serial devices located a distance away from my server closet and the Dominion KSX II. Can I connect these devices to my Raritan switch?

Yes. See *Distances for Serial Devices* (on page 288) for more information.

How do I upgrade the software on my Dominion KSX II?

Use the Firmware Upgrade page to upgrade the firmware for your KSX II unit and all attached D2CIM-VUSB. This page is available in the KSX II Remote Console only.

Are updates to Dominion KSX II software free?

Yes. Currently all software upgrades are free.

Does Dominion KSX II require any additional client software?

No. Dominion KSX II is truly "Plug-and-Play" making installation quick and set-up easy. It is not necessary to buy any additional client software or hardware. In addition, no special networking equipment or design is necessary.

What is the name of the terminal emulation package included with Dominion KSX II?

Raritan Serial Console.

What Authentication mechanisms does the Dominion KSX II support?

Local database, RADIUS, LDAP/S, Active Directory.

Does Dominion KSX II support SNMP?

Yes. Dominion KSX II supports SNMP traps via the Raritan Enterprise MIB.

Does Dominion KSX II support syslog?

Yes. Dominion KSX II supports syslog - to primary and secondary servers.

Can I log every keystroke of a session (input from user and response from a server/device) with a server?

Yes, KSX II supports client-side logging.

Does Dominion KSX II support Telnet?

Yes. Dominion KSX II supports enabling of the telnet daemon on the Dominion KSX II unit. Because telnet sends all information "in the clear", enabling telnet is at the customers own discretion, and telnet is disabled by default when the unit ships from the factory. Raritan strongly suggests the use of SSH as a safer alternative to telnet, since all data is encrypted, including the login sequence.

Can I send an intentional "break" signal to the Sun™ Solaris™ server when using SSH?

Yes.

Can I send an intentional "break" signal to the Sun Solaris server when using a web browser?

Yes, using Raritan Serial Console.

Can I send an intentional "break" signal to the Sun Solaris server when using Telnet?

Yes.

Can I get the buffered off-line data from a serial port when using SSH?

Yes.

Can I get the buffered off-line data from a serial port when using Telnet?

Yes.

Can I use KSX II over a VPN connection?

Yes, KSX II fits into most any network configuration utilizing TCP/IP. KSX II uses standard Internet Protocol (IP) technologies from Layer 1 through Layer 4. Set up the VPN (typically IPSec) connection then start the web-browser and enter the URL for the Dominion device. The session to the Dominion runs transparently over the VPN tunnel.   Traffic can be easily tunneled through standard VPNs.

Can I get the buffered off-line data from a serial port when using a Java™-enabled web-browser?

Yes.

Does Dominion KSX II support local (direct) port access for "crash-cart" applications in a data center?

Yes.

What are the pin-outs of the Dominion KSX II serial ports?

To provide maximum port density and to enable simple UTP (Category 5) cabling, The KSX II provides its serial connections via compact RJ-45 ports. However, no widely adopted industry-standard exists for sending serial data over RJ-45 connections.

The following tables list the RJ-45 pinouts for the RJ-45 connector.

RJ-45 PIN	SIGNAL
1	RTS
2	DTR
3	TxD
4	GND
5	DCD
6	RxD
7	DSR
8	CTS

Go to the Raritan website (www.raritan.com) Support page to find the latest information about the KSX II serial pinouts (RJ-45).

The Dominion KSX II uses the web browser to access serial devices. What are the advantages of Java-enabled web browser access?

For many Solaris/Unix/Linux system administrators, the de facto standard for accessing serial hosts is SSH. However, the SSH clients available for Unix/Linux do not support Apple Macintosh. Additionally, Java-enabled browsers are available on many platforms, including PDAs and handheld PCs. The easy "point-and-click" access offered by Dominion KSX II allows administrators secure access from any Java-enabled web browser.

Universal Virtual Media

What KSX II models support virtual media?

All of the KSX II models support virtual media. It is available standalone and through Raritan's CommandCenter Secure Gateway, Raritan's centralized management unit.

What types of virtual media does the KSX II support?

The KSX II supports the following types of media: internal and USB-connected CD/DVD drives, USB mass storage devices, PC hard drives, and ISO images.

What is required for virtual media?

A KSX II virtual media CIM is required.   There are two of these CIMs: the D2CIM-VUSB and the new D2CIM-DVUSB.

The D2CIM-DVUSB has dual USB connectors and should be purchased by customers who wish to utilize virtual media at the BIOS level. The D2CIM-DVUSB is also required for smart card authentication.

The D2CIM-VUSB has a single USB connector and is for customers who will use virtual media at the OS level.

Both support virtual media sessions to target servers supporting the USB 2.0 interface.

Available in economical 32 and 64 quantity CIM packages, these CIMs support Absolute Mouse Synchronization as well as remote firmware update.

Is virtual media secure?

Yes. Virtual media sessions are secured using AES or RC4 encryption.

USB Profiles

What is a USB profile?

Certain servers require a specifically configured USB interface for USB based services such as virtual media. The USB Profile tailors the KSX II's USB interface to the server to accommodate these server specific characteristics.

Why would I use a USB profile?

USB Profiles are most often required at the BIOS level where there may not be full support for the USB specification when accessing virtual media drives.

However, profiles are sometimes used at the operating system level, for example, for mouse synchronization for Mac® and Linux® servers.

How is a USB profile used?

Individual or groups of ports can be configured by the administrator to use a specific USB profile in the KSX II's Port Configuration pages.

A USB profile can also be selected in the KSX II client when required.

What happens if I don't choose the correct USB profile?

Not choosing the right USB profile for a KVM target server can prevent a mass storage device, mouse, or keyboard from working optimally or working at all.

Do I always need to set a USB profile when I use virtual media?

No, in many cases, the default USB Profile is sufficient when using virtual media at the OS level or operating at the BIOS level without accessing virtual media.

What profiles are available?

See *Available USB Profiles* (on page 105).

How do I know which USB profile is best for a given target server?

The Generic profile is best for the vast majority of target servers. If this profile does not work with a given KVM target server, you can choose the appropriate USB profile in *Available USB Profiles* (on page 105). Select the profile that best matches your target server.

What is the purpose of a BIOS profile?

A BIOS profile has been tailored to match the requirements of a particular server's BIOS that does not implement the full USB specification. The profile enables use of keyboard, mouse, and virtual media at the BIOS level, overcoming the restrictions or limitations of the BIOS.

Do I need a special CIM to use USB profiles?

You must use a D2CIM-VUSB or D2CIM-DVUSB with updated firmware.

Will Raritan provide USB profiles for other target server configurations?

Raritan will provide new USB profiles to suit customer needs. As these profiles become available, they will be included in firmware upgrades.

IPv6 Networking

What is IPv6?

IPv6 is the acronym for "Internet Protocol Version 6". IPv6 is the "next generation" IP protocol which will replace the current IP Version 4 (IPv4) protocol.

IPv6 addresses a number of problems in IPv4, such as the limited number of IPv4 addresses. It also improves IPv4 in areas such as routing and network auto-configuration. IPv6 is expected to gradually replace IPv4, with the two coexisting for a number of years.

IPv6 helps one of the largest headaches of an IP network from the administrator's point of view; configuring and maintaining an IP network.

Why does the KSX II support IPv6 networking?

US government agencies and the Department of Defense are now mandated to purchase IPv6 compatible products. In addition, many enterprises and foreign countries such as China will be transitioning to IPv6 over the next several years.

What is "dual stack" and why is it required?

Dual stack is the ability to simultaneously support both IPv4 and IPv6 protocols. Given the gradual transition from IPv4 to IPv6, dual stack is a fundamental requirement for IPv6 support.

How do I enable IPv6 on the KSX II?

Use the Network Settings page, available from the Device Settings menu in KSX II. Enable IPv6 addressing and choose manual or auto-configuration. You must also enable it in MPC.

What if I have an external server with an IPv6 address that I want to use with my KSX II?

The KSX II can access external servers via their IPv6 addresses, for example, an SNMP Manager, Syslog server, or LDAP server.

Using the KSX II's dual-stack architecture, these external servers can be accessed via (1) an IPv4 address, (2) IPv6 address or (3) hostname. So the KSX II supports the mixed IPv4/IPv6 environment many customers will have.

Does the Dominion KX I support IPv6?

No, the Dominion KX I does not support IPv6 addresses.

What if my network doesn't support IPv6?

The KSX II's default networking is set at the factory for IPv4 only. When you are ready to use IPv6, then follow the above instructions to enable IPv6/IPv4 dual stack operation.

Where can I get more information on IPv6?

See www.ipv6.org for general information on IPv6. The KSX II User Guide describes the KSX II's support for IPv6.

Remote Access

How many users can remotely access servers on each KSX II?

Up to 8 KVM users can share one KVM channel and up to 8 serial users can share 8 serial channels.

Can two people look at the same server at the same time?

Yes, up to eight people can access and control any single server at the same time.

Can two people access the same server, one remotely and one from the local port?

Yes, the local port is completely independent of the remote "ports." The local port can access the same server using the PC-Share feature.

In order to access KSX II from a client, what hardware, software or network configuration is required?

Because the KSX II is completely web-accessible, it doesn't require installation of proprietary software on clients used for access. The browser does have to be Java enabled, though.

The KSX II can be accessed through major web browsers including: Internet Explorer, Mozilla and Firefox. The KSX II can now be accessed on Windows, Linux, Sun Solaris and Macintosh desktops, via Raritan's Java-based Multi-Platform Client (MPC), RSC and the new Virtual KVM Client.

When using an SSH client, the customer has to provide an SSH client. In some operating systems, like Linux, an SSH client is included in the distribution. Also, OpenSSH.org has an SSH client.

The KSX II administrators can also perform remote management (set passwords and security, rename servers, change IP address, and so forth) using a convenient browser-based interface.

What is the file size of the Virtual KVM Client applet that is used to access the KSX II? How long does it take to retrieve?

The Virtual KVM Client applet used to access the KSX II is approximately 500KB in size. The following chart describes the approximate time required to retrieve the KSX II's applet at different network speeds:

Speed	Description	Time
100Mbps	Theoretical 100Mbit network speed	0.05 seconds

Speed	Description	Time
60Mbps	Likely practical 100Mbit network speed	0.08 seconds
10Mbps	Theoretical 10Mbit network speed	.4 seconds
6Mbps	Likely practical 10Mbit network speed	.8 seconds
512Kbps	Cable modem download speed (typical)	8 seconds

How do I access servers connected to the KSX II if the network ever becomes unavailable?

The KSX II offers an internal modem port.   With this modem servers can still be remotely accessed in the event of a network emergency. Furthermore, the KSX II's local ports always allow access to servers from the rack, regardless of the network condition.

Do you have a non-Windows® client?

Yes. The Virtual KVM Client, Raritan Serial Console (RSC) and the Multi-Platform Client (MPC) allow non-Windows users to connect to KVM target servers through the KSX II switches. MPC can be run via web browsers and standalone.

Sometimes during a Virtual KVM Client session, the Alt key appears to get stuck. What should I do?

This usually occurs in situations when the Alt key is held and not released. For instance, continuing to press the Alt key while pressing the space bar might cause the focus to change from the target server to the client PC. The local operating system then interprets this key combination and consequently triggers the action for this key combination in the active window (the client PC).

Ethernet and IP Networking

Does the KSX II offer dual gigabit Ethernet ports to provide redundant fail-over, or load balancing?

Yes. The KSX II features dual gigabit Ethernet ports to provide redundant failover capabilities. Should the primary Ethernet port (or the switch/router to which it is connected) fail, the KSX II will failover to the secondary network port with the same IP address, ensuring that server operations are not disrupted. Note that automatic failover must be enabled by the administrator.

How much bandwidth does the KSX II require?

The KSX II offers next generation KVM-over-IP technology - the very best video compression available. Raritan has received numerous technical awards confirming its high video quality transmissions and the low bandwidth utilization.

Raritan pioneered the KVM-over-IP functionality that allows users to tailor their video parameters to conserve network bandwidth. For instance, when connecting to the KSX II through a dial-up modem connection, video transmissions can be scaled to grayscale - allowing users to be fully productive while ensuring high performance.

With that in mind, the following data refers to the KSX II at its default video settings - again, these settings can be tailored to a specific environment. They can be increased to provide even higher quality video (color depth), or decreased to optimize for low-speed connections.

As a general rule, a conservative estimate for bandwidth utilization (at the KSX II's default settings) is approximately 0.5Mbit/second per active KVM user (connected to and using a server), with very occasional spikes up to 2MBit/second. This is a very conservative estimate because bandwidth utilization will typically be even lower.

Bandwidth required by each video transmission depends on what task is being performed on the managed server. The more the screen changes, the more bandwidth is utilized. The table below summarizes some use cases and the required bandwidth utilization at the KSX II's default settings on a 10Mbit/s network:

Use case	Required bandwidth
Idle Windows Desktop	0 Mbps
Move Cursor Around Desktop	0.18Mbps

Use case	Required bandwidth
Idle Windows Desktop	0 Mbps
Move Static 400x600 Window/Dialog	0.35Mbps
Navigate Start Menu	0.49Mbps
Scroll an Entire Page of Text	1.23Mbps
Run 3D Maze Screensaver	1.55Mbps

What is the slowest connection (lowest bandwidth) over which the KSX II can operate?

33Kbps or above is recommended for acceptable KSX II performance over a modem connection.

What is the speed of the KSX II's Ethernet interfaces?

The KSX II supports two 10/100/1000 speed Ethernet interfaces, with configurable speed and duplex settings (either auto-detected or manually set).

Can I access the KSX II over a wireless connection?

Yes. The KSX II not only uses standard Ethernet, but also very conservative bandwidth with very high quality video. Thus, if a wireless client has network connectivity to the KSX II, servers can be configured and managed at BIOS-level wirelessly.

Can the KSX II be used over the WAN (Internet), or just over the corporate LAN?

Whether via a fast corporate LAN, the less predictable WAN (Internet), cable modem or dial-up modem, the KSX II's KVM-over-IP technology can accommodate the connection.

How many TCP ports must be open on my firewall in order to enable network access to the KSX II? Are these ports configurable?

Only one. The KSX II protects network security by only requiring access to a single TCP port to operate. This port is completely configurable for additional security.

Note that, of course, to use the KSX II's optional web browser capability, the standard HTTPS port 443 must also be open.

Can the KSX II be used with CITRIX?

The KSX II may work with remote access products like CITRIX if configured appropriately, but Raritan cannot guarantee it will work with acceptable performance. Products like CITRIX utilize video redirection technologies similar in concept to digital KVM switches so that two KVM-over-IP technologies are being used simultaneously.

Does the KSX II require an external authentication server to operate?

No, the KSX II is a completely self-sufficient. After assigning an IP address to a KSX II, it is ready to use - with web browser and authentication capabilities completely built-in.

If an external authentication server (such as LDAP/LDAPS, Active Directory, RADIUS, and so forth) is used, the KSX II allows this as well, and will even failover to its own internal authentication should the external authentication server become unavailable. In this way, the KSX II's design philosophy is optimized to provide ease of installation, complete independence from any external server, and maximum flexibility.

Can the KSX II use DHCP?

DHCP addressing can be used, however, Raritan recommends fixed addressing since the KSX II is an infrastructure device and can be accessed and administered more effectively with a fixed IP address.

I'm having problems connecting to the KSX II over my IP network. What could be the problem?

The KSX II relies on your LAN/WAN network. Some possible problems include:

- Ethernet autonegotiation - On some networks, 10/100 autonegotiation does not work properly and the KSX II unit must be set to 100MB/full duplex or the appropriate choice for its network.

- Duplicate IP address - If the IP address of the KSX II is the same as another device, network connectivity may be inconsistent.

- Port 5000 conflicts - If another device is using port 5000, the KSX II default port must be changed (or the other device must be changed).

When changing the IP address of the KSX II or swapping in a new KSX II, sufficient time must be allowed for its IP and MAC addresses to be known throughout the Layer 2 and Layer 3 networks.

Servers

Does the KSX II depend on a Windows® server to operate?

No. The KSX II is completely independent. Even if a user chooses to configure the KSX II to authenticate against an Active Directory server - if that Active Directory server becomes unavailable, the KSX II's own authentication will be activated and fully functional.

Do I need to install a web server such as Microsoft® Internet Information Services (IIS) in order to use the KSX II's web browser capability?

No. The KSX II is a completely self-sufficient device. After assigning an IP address to the KSX II, it's ready to use since it comes with web browser and authentication capabilities completely built-in.

What software do I have to install in order to access the KSX II from a particular workstation?

None. The KSX II can be accessed completely via a web browser. However, there is an optional installed client provided on Raritan's website (www.raritan.com), which is required for modem connections. A Java-based client is now available for non-Windows users.

Blade Servers

Can I connect blade servers to the KSX II?

Yes. The KSX II supports popular blade server models from the leading blade server manufacturers: HP®, IBM® and Dell®.

Which blade servers are supported?

The following models are supported:

- Dell® PowerEdge® 1855, 1955 and M1000e
- HP BladeSystem c3000 and c7000
- IBM® BladeCenter® H and E

  Note: IBM BladeCenter Model S, T, and HT are handled using the IBM (Other) selection.

Are the Paragon Blade CIMs used?

No, the Paragon II Blade CIM will not work with the KSX II.

Which CIM should I use?

It depends on the type of KVM ports on the specific make and model of the blade server you are using. The following CIMs are supported: DCIM-PS2, DCIM-USBG2, D2CIM-VUSB and D2CIM-DVUSB.

What types of access and control are available?

The KSX II provides automated & secure KVM access: (1) at-the-rack, (2) remotely over IP, (3) via CommandCenter and (4) by modem.

Do I have to use hotkeys to switch between blades?

Some blade servers require you to use hotkeys to switch between blades. With the KSX II, you don't have to use these hotkeys. Just click on the name of the blade server and the KSX II will automatically switch to that blade without the explicit use of the hotkey.

Can I access the blade server's management module?

Yes, you can define the URL of the management module and access it from the KSX II or from CC-SG. If configured, one-click access is available.

How many blade servers can I connect to a KSX II?

For performance and reliability reasons, you can connect up to 8 blade chassis to a KX II (regardless of model) or up to 4 for a KSX II.

For KX II's, Raritan recommends connecting up to two times the number of remote connections supported by the device. For example, with a KX2-216 with two remote channels, we recommend connecting up to 4 blade server chassis. You can of course connect individual servers to the remaining server ports.

I'm an SMB customer with a few KSX II's. Must I use your CC-SG management station?

No, you don't have to. SMB customers are not required to use CC-SG to use the new blade features.

I'm an enterprise customer using CC-SG. Can I access blade servers via CC-SG?

Yes. Once blade servers are configured on the KSX II, the CC-SG user can access them via KVM connections. In addition the blade servers are organized by chassis as well as CC-SG custom views.

What if I want in-band or embedded KVM access?

Yes, in-band and embedded access to blade servers can be configured within CC-SG.

I'm running VMware on some of my blade servers. Is this supported?

Yes, with CC-SG you can display and access virtual machines running on blade servers.

Is virtual media supported?

We support VM on IBM BladeCenter® Model H and E with the D2CIM - DVUSB.

Is Absolute Mouse Synchronization supported?

Servers with internal KVM switches inside the blade chassis typically do not support absolute mouse technology. For HP Blade and some Dell blade servers, the CIM is connected to each blade, so absolute mouse is supported if the underlying OS running on the blade does.

Is blade access secure?

Yes, blade access uses all of the standard KSX II security features such as 128 bit or 256 bit encryption. In addition, there are blade-specific security features such as per blade access permissions and hot key-blocking that eliminates un-authorized access.

Installation

Besides the device itself, what do I need to order from Raritan to install the KSX II?

Each server that connects to the KSX II requires a Dominion Computer Interface Module (CIM), a serial cable adapter, and an adapter that connects directly to the keyboard, video, and mouse ports of the server.

What kind of Cat5 cabling should be used in my installation?

Each server that connects to the KSX II requires a Dominion Computer Interface Module (CIM), a serial cable adapter, and an adapter that connects directly to the keyboard, video, and mouse ports of the server.

What types of servers can be connected to the KSX II?

The KSX II is completely vendor independent. Any server with standard-compliant keyboard, video, and mouse ports can be connected.

How do I connect servers to the KSX II?

See Connecting to a KVM Target Server.

How far can my servers be from the KSX II?

See *Distances for Serial Devices* (on page 288) and *Target Server Connection Distance and Video Resolution* (on page 288).

For the new D2CIM-VUSB and D2CIM-DVUSB CIMs that support virtual media and Absolute Mouse Synchronization, a 100 (30 m) foot range is recommended.

Some operating systems lock up when I disconnect a keyboard or mouse during operation. What prevents servers connected to the KSX II from locking up when I switch away from them?

Each Dominion computer interface module (DCIM) dongle acts as a virtual keyboard and mouse to the server to which it is connected. This technology is called KME (keyboard/mouse emulation). Raritan's KME technology is data center grade, battle-tested, and far more reliable than that found in lower-end KVM switches: it incorporates more than 15 years of experience and has been deployed to millions of servers worldwide.

Are there any agents that must be installed on servers connected to the KSX II?

Servers connected to the KSX II do not require any software agents to be installed, because the KSX II connects directly via hardware to servers' keyboard, video, and mouse ports.

How many servers can be connected to each KSX II device?

The KSX II models range from 4 to 8 server ports in a 1U chassis. This is the industry's highest digital KVM switch port density.

What happens if I disconnect a server from the KSX II and reconnect it to another KSX II device, or connect it to a different port on the same KSX II device?

The KSX II will automatically update the server port names when servers are moved from port to port. This automatic update does not just affect the local access port, but propagates to all remote clients and the optional CommandCenter Secure Gateway management device.

Both serial and KVM ports can be moved without encountering problems. However, once disconnected, the name of a KVM will be retained but the name for a serial port will not be.

Local Port

Can I access my servers directly from the rack?

Yes. At the rack, the KSX II functions just like a traditional KVM switch - allowing control of up to 16 servers using a single keyboard, monitor, and mouse.

When I am using the local port, do I prevent other users from accessing servers remotely?

No. The KSX II local port has a completely independent access path to the servers. This means a user can access servers locally at the rack without compromising the number of users that access the rack remotely at the same time.

Can I use a USB keyboard or mouse at the local port?

Yes. The KSX II offers both PS/2 and USB keyboard and mouse ports on the local port. Note that the USB ports are USB v1.1, and support keyboards and mice only, not USB devices such as scanners or printers.

Is there an Onscreen Display (OSD) for local, at-the-rack access?

Yes, but the KSX II's at-the-rack access goes way beyond conventional OSDs. Featuring the industry's first browser-based interface for at-the-rack access, the KSX II's local port uses the same interface for local and remote access. Moreover, most administrative functions are available at-the-rack.

How do I select between servers while using the local port?

The local port displays the connected servers using the same user interface as the remote client.   Connect to a server with a simple click of the mouse.

How do I ensure that only authorized users can access servers from the local port?

Users attempting to use the local port must pass the same level of authentication as those accessing remotely. This means that:

- If the KSX II is configured to interact with an external RADIUS, LDAP/LDAPS or Active Directory server, users attempting to access the local port will authenticate against the same server.
- If the external authentication servers are unavailable, the KSX II fails-over to its own internal authentication database.

The KSX II has its own standalone authentication, enabling instant, out-of-the-box installation.

If I use the local port to change the name of a connected server, does this change propagate to remote access clients as well? Does it propagate to the optional CommandCenter device?

Yes. The local port presentation is identical and completely in sync with remote access clients, as well as Raritan's optional CommandCenter Secure Gateway management device. To be clear, if the name of a server via the KSX II onscreen display is changed, this updates all remote clients and external management servers in real-time.

If I use the KSX II's remote administration tools to change the name of a connected server, does that change propagate to the local port as well?

Yes. The local port presentation is identical and completely in sync with remote access clients. To be clear, if the name of a server via the KSX II onscreen display is changed, this updates all remote clients and external management servers in real-time.

Sometimes I see "shadows" on the local port user interface. Why does that occur?

This shadow/ghosting effect may occur with LCD monitors that have been on for long periods. The LCD properties and the electrical/static charge can produce these effects when the screen is on for a long time.

Power Control

Does the power supply used by the KSX II automatically detect voltage settings?

Yes. The KSX II's power supply can be used in AC voltage ranges from 100-240 volts, at 50-60 Hz.

What type of power control capabilities does the KSX II offer?

Raritan's Remote Power Control power strips can be connected to the KSX II to provide power control of the KVM target servers. After a simple one-time configuration step, just right click the server name to power on, off, or recycle a hung server. Note that a hard reboot provides the physical equivalent of unplugging the server from the AC power line, and reinserting the plug.

Does the KSX II support servers with multiple power supplies? What if each power supply is connected to a different rack PDU (power strip)?

Yes. The KSX II can be easily configured to support multiple power supplies connected to multiple power strips. Two (2) power strips can be connected to a KSX II device. Four power supplies can be connected per target server to multiple power strips.

Does remote power control require any special server configuration?

Some servers ship with default BIOS settings such that the server does not automatically restart after losing and regaining power. For these servers, see the server's documentation to change this setting.

What type of rack PDUs (power strips) does the KSX II support?

To take advantage of the KSX II's integrated power control user interface and, more importantly, integrated security, use Raritan's Remote Power Control (RPC) power strips or Dominion PX power strips. A CAT5 cable is used to connect the PDU port on the KSX II to a PX or RPC unit.

The Dominion PX is an intelligent power distribution unit that allows you to reboot remote servers and other network devices, and monitor power in the data center, through Raritan's KVM switches and Secure Console Servers.

Scalability

How do I connect multiple KSX II devices together into one solution?

Multiple KSX II devices do not need to be physically connected together. Instead, each KSX II device connects to the network. They automatically work together as a single solution if deployed with Raritan's optional CommandCenter Secure Gateway (CC-SG) management unit. CC-SG acts as a single access point for remote access and management. CC-SG offers a significant set of convenient tools, such as consolidated configuration, consolidated firmware update, and a single authentication and authorization database.

In addition, CC-SG enables sophisticated server sorting, permissions, and access. If deployment of Raritan's CC-SG management unit isn't an option, multiple KSX II devices still interoperate and scale automatically. The KSX II's remote user interface and the Multi-Platform Client will automatically discover KSX II devices. Non-discovered KSX II devices can be accessed via a user-created profile.

Can I connect an existing analog KVM switch to the KSX II?

Yes. Analog KVM switches can be connected to one of the KSX II's server ports. Simply use a D2CIM-DVUSB or D2CIM-VUSB and attach it to the user ports of the existing analog KVM switch. Please Note that analog KVM switches vary in their specifications and Raritan cannot guarantee the interoperability of any particular third-party analog KVM switch. Contact Raritan technical support for further information.

Security

Is the KSX II FIPS 140-2 Certified?

The KX II 2.2.0 and later, and the KSX II 2.3.0 and later, provides users with the option to use an embedded FIPS 140-2-validated cryptographic module running on a Linux platform per FIPS 140-2 implementation guidelines. This cryptographic module is used for encryption of KVM session traffic consisting of video, keyboard, mouse, virtual media and smart card data.

What kind of encryption does the KSX II use?

The KSX II uses industry-standard (and extremely secure) 128-bit RC4, 128 bit AES or 256bit AES encryption, both in its SSL communications as well as its own data stream. Literally no data is transmitted between remote clients and KSX II that is not completely secured by encryption.

Does the KSX II support AES encryption as recommended by the US Government's NIST and FIPs standards?

The KSX II utilizes the Advanced Encryption Standard (AES) encryption for added security.

AES is a US government approved cryptographic algorithm that is recommended by the National Institute of Standards and Technology (NIST) in the FIPS Standard 197.

Does the KSX II allow encryption of video data? Or does it only encrypt keyboard and mouse data?

Unlike competing solutions, which only encrypt keyboard and mouse data, the KSX II does not compromise security; it allows encryption of keyboard, mouse and video data.

How does the KSX II integrate with external authentication servers such as Active Directory®, RADIUS, or LDAP/S?

Through a very simple configuration, the KSX II can be set to forward all authentication requests to an external server such as LDAP/S, Active Directory, or RADIUS. For each authenticated user, the KSX II receives from the authentication server the user group to which that user belongs. The KSX II then determines the user's access permissions depending on the user group to which he or she belongs.

How are usernames and passwords stored?

Should the KSX II's internal authentication capabilities be used, all sensitive information such as usernames and passwords are stored in an encrypted format. Literally no one, including Raritan technical support or Product Engineering departments, can retrieve those usernames and passwords.

Does the KSX II support strong password?

Yes, the KSX II has administrator-configurable, strong password checking to ensure that user-created passwords meet corporate and/or government standards and are resistant to brute force hacking.

If the KSX II Encryption Mode is set to Auto, what level of encryption is achieved?

The KSX II has the ability to support AES-256. For this to happen, Java unlimited strength policy files have to be loaded on the client machine. Once this is enabled, the encryption level that is auto-negotiated when the mode is set to AUTO is as.

Browser	Encryption Level
Internet Explorer 6, 7 and 8	AES-128
Firefox 1.5, 2.0 3.x	AES-256
Safari 2.0.4	AES-256

Does the KSX II support a configurable security banner?

Yes. For government, military and other security conscious customers requiring a security message before user login, the KSX II can display a user-configurable banner message and optionally require acceptance.

Smart Cards and CAC Authentication

Does the KSX II support smart card and CAC authentication?

Yes, smart cards and DoD Common Access Card (CAC) authentication to target servers is supported in release KX II 2.1.10 and later, and KSX II 2.3.0 and later.

What KSX II models support smart cards/CAC?

All KSX II models are supported. The Dominion KX II-101 does not currently support smart cards and CAC.

Do enterprise and SMB customers use smart cards, too?

Yes. However, the most aggressive deployment of smart cards is in the U.S. federal government.

What CIMs support smart cards/CAC?

The D2CIM-DVUSB is required. This CIM must be upgraded with the release 2.1.10 and later of the firmware, and KSX II 2.3.0 and later.

What firmware version is required?

The KX II release 2.1.10 and later or and KSX II 2.3.0 and later are required.

What smart card readers are supported?

The required reader standards are USB CCID and PC/SC. See *Supported and Unsupported Smart Card Readers* (on page 282).

Can smart card/CAC authentication work on the local port and via Command Center?

Yes. For the local port, connect a compatible smart card reader to the USB port of the KSX II.

Are the Paragon smart card enabled UST and CIM used?

No, the P2-EUST/C and P2CIM-AUSB-C are not part of the KSX II solution.

Managability

Can the KSX II be remotely managed and configured via web browser?

Yes, the KSX II can be completely configured remotely via web browser. Note that this does require that the workstation have an appropriate Java Runtime Environment (JRE) version installed.

Besides the initial setting of the KSX II's IP address, everything about the solution can be completely set up over the network. (In fact, using a crossover Ethernet cable and the KSX II's default IP address, you can even configure the initial settings via web browser.)

Can I backup and restore the KSX II's configuration?

Yes, the KSX II's device and user configurations can be completely backed up for later restoration in the event of a catastrophe.

The KSX II's backup and restore functionality can be used remotely over the network or via the Remote Console.

What auditing or logging does the KSX II offer?

For complete accountability, the KSX II logs all major user and system events with a date and time stamp. For instance, reported events include (but are not limited to): user login, user log off, user access of a particular server, unsuccessful login, configuration changes, and so forth.

Can the KSX II integrate with Syslog?

Yes. In addition to the KSX II's own internal logging capabilities, the KSX II can send all logged events to a centralized Syslog server.

Can the KSX II integrate with SNMP?

Yes. In addition to the KSX II's own internal logging capabilities, the KSX II can send SNMP traps to SNMP management systems like HP OpenView and Raritan's CC-NOC.

Can the KSX II's internal clock be synchronized with a timeserver?

Yes, the KSX II supports the industry-standard NTP protocol for synchronization with either a corporate timeserver or with any public timeserver (assuming that outbound NTP requests are allowed through the corporate firewall).

Miscellaneous

What is the KSX II's default IP address?

192.168.0.192

What is the KSX II's default user name and password?

The KSX II's default user name is admin and the default password is raritan [all lower case]. However, for the highest level of security, the KSX II forces the administrator to change the KSX II default administrative user name and password when the unit is first booted up.

I changed and subsequently forgot the KSX II's administrative password; can you retrieve it for me?

The KSX II contains a hardware reset button that can be used to factory reset the device, which will reset the administrative password on the device.

I am logged into the KSX II using Firefox®, and I opened another Firefox browser. I am automatically logged into the same KSX II with the second Firefox browser. Is this right?

Yes, this is correct behavior and is the direct result of how browsers and cookies function.

I am logged into the KSX II using Firefox and I attempt to log into another KSX II using another Firefox browser session from the same client. I am logged off of both KSX IIs; is this correct behavior?

Yes, to access two different KSX II devices either close the first session or use another client PC.

Index

A

A. AC Power • 25
Absolute Mouse Mode • 73
Accessing a Target Server • 250
Accessing Telnet from a Windows PC • 228
Accessing the KSX II Using CLI • 227
Accessing Virtual Media on a Windows 2000 Server Using a D2CIM-VUSB • 312
Active KVM Client (AKC) • 4, 39, 80
Adding a New User • 121
Adding a New User Group • 114, 121
Adding Attributes to the Class • 296
Adding, Deleting and Editing Favorites • 51
Adjusting Video Settings • 64
Administering the KSX II Console Server Configuration Commands • 236
AES 256 Prerequisites and Supported Configurations for Java • 301
AKC Supported .NET Framework, Operating Systems and Browsers • 81
Apple Macintosh Settings • 24
Assigning a Name to the PX • 159
Assigning an IP Address • 31
Associating KVM and Serial Target Servers to Outlets (Port Page) • 159
Audit Log • 205, 253, 254
Authentication Settings • 123
Auto-Sense Video Settings • 64
Available Resolutions • 244
Available USB Profiles • 105, 310, 323

B

B. Network Port • 26
Backup and Restore • 173, 207
Blade Chassis Sample URL Formats • 166, 167, 169, 171, 180
Blade Servers • 332
Building a Keyboard Macro • 61

C

C. Local User Port (Local PC) and Local Admin Port • 26
Calibrating Color • 64
CC Unmanage • 216
CC-SG • 313
CD-ROM/DVD-ROM/ISO Images • 97, 101

Certified Modems for UNIX, Linux and MPC • 256
Changing a Password • 134
Changing a USB Profile when Using a Smart Card Reader • 311
Changing the Default Password • 30
Changing the Keyboard Layout Code (Sun Targets) • 37
Changing the Maximum Refresh Rate • 69
Checking Your Browser for AES Encryption • 194, 196
Choosing USB Profiles • 56
CIM Compatibility • 105
CIMs • 311
CLI Commands • 226, 234
CLI Prompts • 234
CLI Syntax -Tips and Shortcuts • 232
Client Dial-Up Networking Configuration • 258
Command Line Interface (CLI) • 39, 225
Common Commands for All Command Line Interface Levels • 232
Completion of Commands • 231
Computer Interface Modules (CIMs) • 105, 274
Conditions when Read/Write is Not Available • 100, 101
Configuring Blade Chassis • 161
Configuring Date/Time Settings • 148
Configuring Direct Port Access via Telnet, IP Address or SSH • 34, 142, 143
Configuring Event Management - Destinations • 152
Configuring Event Management Settings • 150, 152
Configuring IP Access Control • 198
Configuring KSX II Local Port Settings • 183
Configuring Modem Settings • 147
Configuring Network • 236
Configuring Ports • 155
Configuring USB Profiles (Port Page) • 111, 170, 181
Connect Commands • 238
Connect Key Examples • 184, 247
Connecting to a KVM Target Server • 53, 56, 57
Connecting to Virtual Media • 100
Connection Information • 60
Connection Properties • 58
Connectivity • 286, 290

K

Key Combinations and the Java Runtime Environment (JRE) • 306
Keyboard Language Preference (Fedora Linux Clients) • 305
Keyboard Macros • 60
Keyboard Options • 60
Keyboards • 304
KSX II Client Applications • 5
KSX II Console Layout • 42
KSX II Help • 5
KSX II Local Console • 240
  KSX II Devices • 39
KSX II Local Console Factory Reset • 253
KSX II Local Console Interface • 241
KSX II Local Console Local Port Settings • 247, 250, 251
KSX II Local Console Support Languages • 280
KSX II Overview • 2
KSX II Remote Console Interface • 39, 40
KSX II Serial RJ-45 Pinouts • 291
KSX II to KSX II Guidelines • 276
KSX II to Paragon II Guidelines • 277
KVM Properties • 286

L

LAN Interface Settings • 33, 138
Launching MPC from a Web Browser • 82
Launching the KSX II Remote Console • 40
Left Panel • 43
Linux Settings (Red Hat 4) • 19
Local Console Smart Card Access • 76, 242
Local Console USB Profile Options • 243
Local Drives • 100
Local Port • 337
Local Port Administration • 250
Local Port Requirements • 283
Local Serial Port Connection to the KSX II • 228
Logging a User Off (Force Logoff) • 4, 122
Logging On • 229
Logging Out • 51
Login Limitations • 189, 190
Low Bandwidth KVM Settings • 257

M

Macintosh Keyboard • 307
Maintenance • 204

Maintenance Features (Local/Remote Console) • 204
Make Linux Settings Permanent • 20
Make UNIX Settings Permanent • 21
Managability • 344
Manage Favorites Page • 49
Managing Favorites • 44, 48
Minimum System Requirements • 242, 283
Miscellaneous • 345
Modem Configuration • 10, 256
Modifying an Existing User • 122
Modifying an Existing User Group • 119
Modifying and Removing Keyboard Macros • 62
Mouse Modes when Using the Mac OS-X USB Profile with a DCIM-VUSB • 112, 181
Mouse Options • 69
Mouse Pointer Synchronization • 70
Mouse Pointer Synchronization (Fedora) • 308
Mouse Settings • 15
Moving Between Ports of the KSX II • 313
Multi-Platform Client (MPC) • 39, 82

N

Name Command • 237
Naming Target Servers • 33
Navigation of the CLI • 230, 231
Network Basic Settings • 136
Network Interface Page • 219
Network Settings • 25, 33, 135, 138, 287
Network Speed Settings • 139, 289
Network Statistics Page • 219
Non-US Keyboards • 304
Note on Microsoft Active Directory • 36
Note to CC-SG Users • 36

O

Opening RSC from the Remote Console • 84
Operating System Mouse and Video Settings • 16
Overview • 14, 53, 80, 86, 91, 104, 226, 240, 301

P

Package Contents • 13
Permissions • 115, 116
Physical Specifications • 269
Ping Host Page • 221
Port Access Page • 4, 45
Port Access Page (Local Console Server Display) • 245

▶ U.S./Canada/Latin America

Monday - Friday
8 a.m. - 6 p.m. ET
Phone: 800-724-8090 or 732-764-8886
For CommandCenter NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

▶ China

Beijing
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

▶ India

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

▶ Japan

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-3523-5991
Email: support.japan@raritan.com

▶ Europe

Europe
Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom
Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France
Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany
Monday - Friday
8:30 a.m. - 5:30 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0
Email: rg-support@raritan.com

▶ Melbourne, Australia

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

▶ Taiwan

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: support.apac@raritan.com